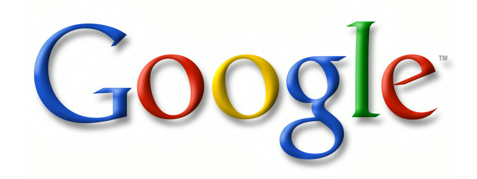
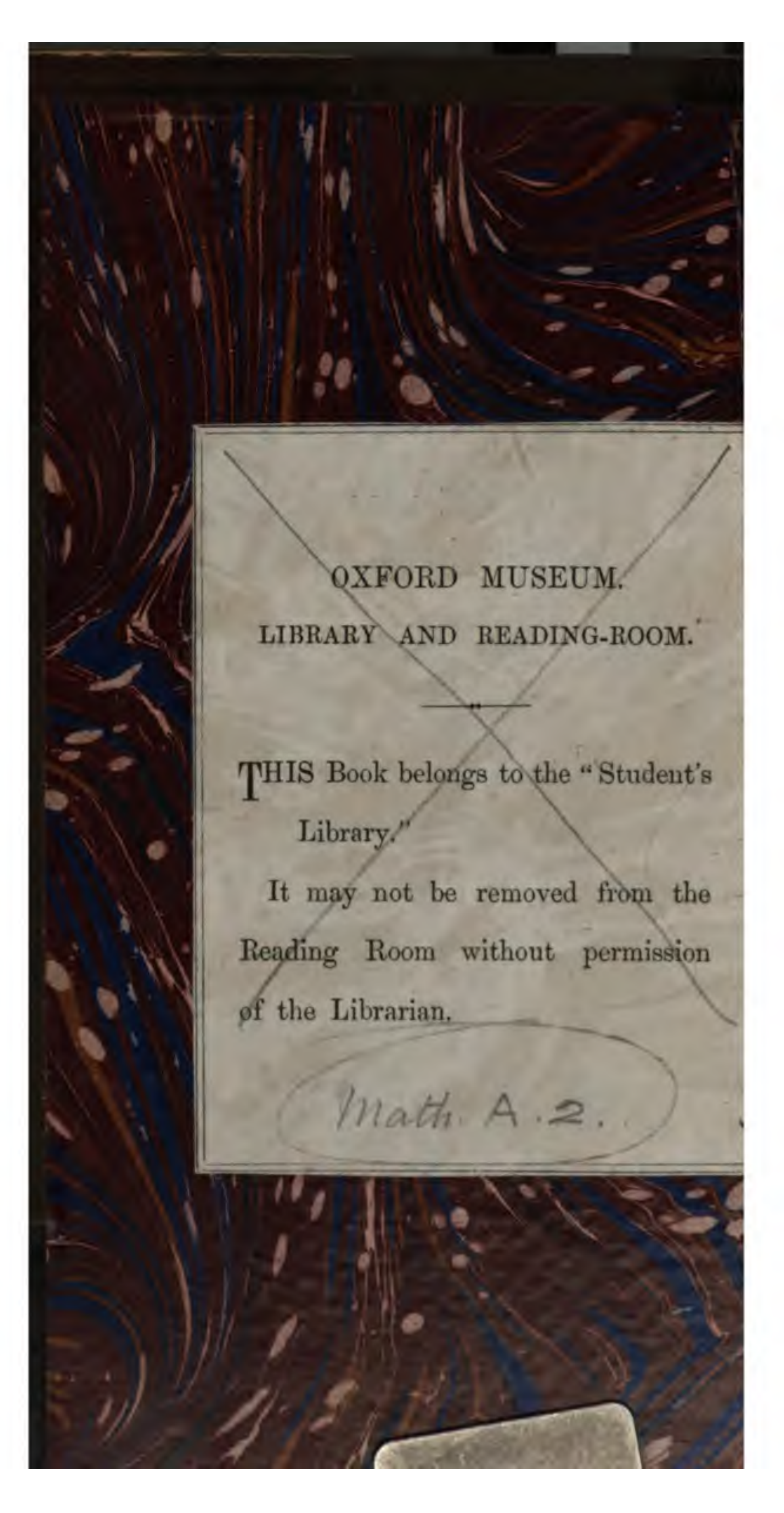
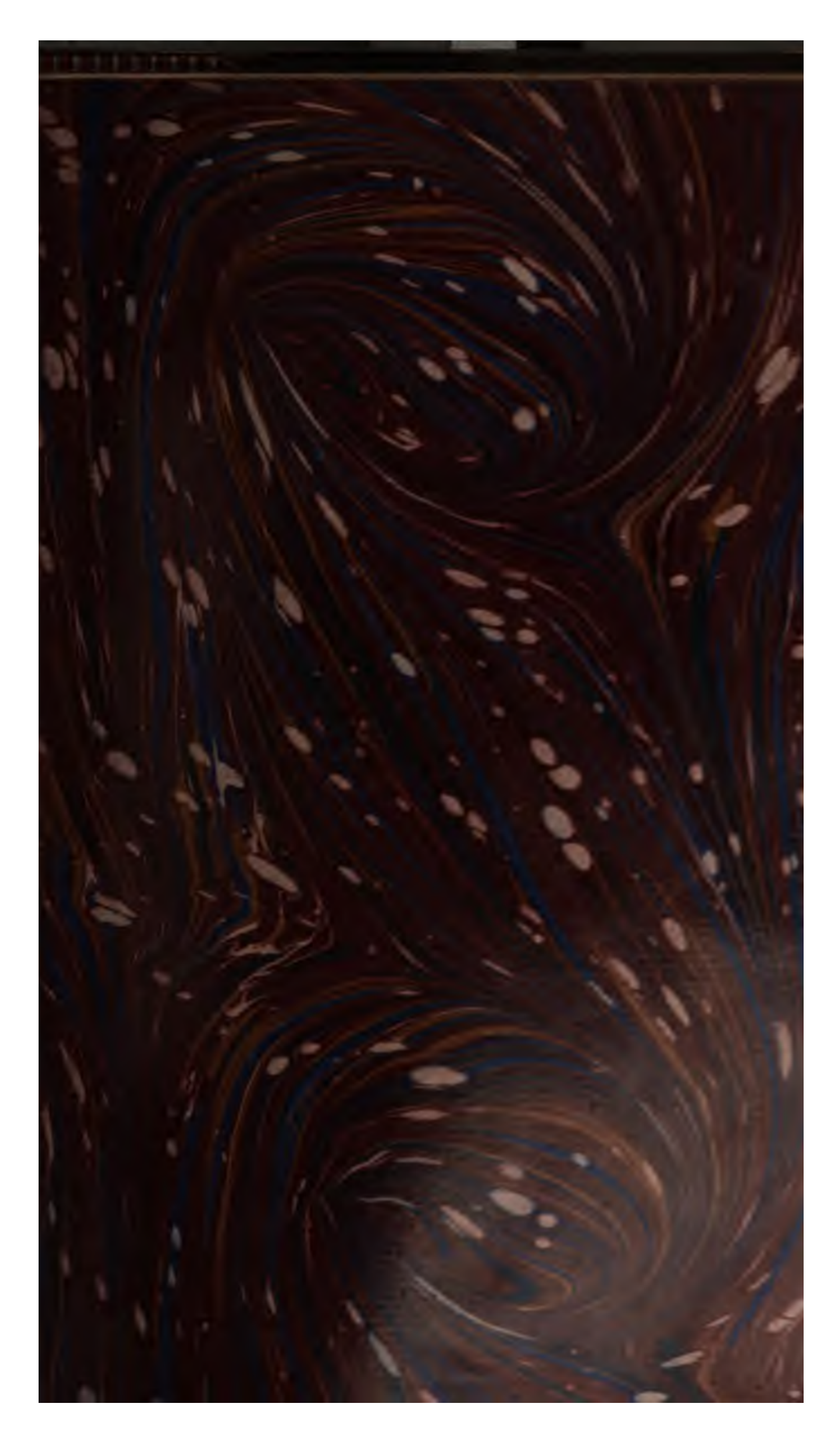







600047024N

COURS
D'ALGÈBRE SUPÉRIEURE

COURS

D'ALGÈBRE SUPÉRIEURE

PAR

J.-A. SERRET,

MEMBRE DE L'INSTITUT ET DU BUREAU DES LONGITUDES.

CINQUIÈME ÉDITION.

TOME SECOND.



PARIS,

GAUTHIER-VILLARS, IMPRIMEUR-LIBRAIRE

DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE.

SUCCESSEUR DE MALLET-BACHELIER,

Quai des Augustins, 55.

1885



TABLE DES MATIÈRES

DU TOME SECOND.

Pages

INTRODUCTION.. 1

SECTION III.

LES PROPRIÉTÉS DES NOMBRES ENTIERS.

CHAPITRE PREMIER.

DES CONGRUENCES.

Des nombres congrus ou équivalents........................ 5
Du nombre qui exprime combien il y a de nombres premiers à un nombre donné et non supérieurs à ce nombre................ 9
Des congruences en général................................ 14
Des congruences du premier degré.......................... 16
Sur le nombre des racines de la congruence $x^2 - 1 \equiv 0$ (mod. M). 24
Théorème de Fermat.. 30
Théorème de Wilson.. 32
Théorème de Fermat généralisé............................. 36
Théorème de Wilson généralisé............................. 37
Des congruences dont le module est un nombre premier......... 39
Nouvelle démonstration du théorème de Wilson................ 46

CHAPITRE II.

DES RÉSIDUS DES PUISSANCES ET DES CONGRUENCES BINOMES.

Des nombres qui appartiennent à un exposant donné relativement à un module donné.. 47
Des racines primitives..................................... 50

Pages.

Des racines primitives, dans le cas où le module est un nombre premier impair 53
Autre manière de présenter les résultats qui précèdent 57
Théorème relatif aux résidus des puissances dont le degré est un diviseur de $p-1$ 64
Recherche des racines primitives d'un nombre premier 68
Des racines primitives dans le cas où le module est égal à une puissance d'un nombre premier impair ou égal au double d'une telle puissance 77
De la congruence $x^t - 1 \equiv 0$ (mod. M), dans le cas où M est égal à une puissance d'un nombre premier impair ou égal au double d'une telle puissance 83
Du module 2^ν 85
De la congruence $x^t - 1 \equiv 0$ (mod. 2^ν) 88
De la congruence $x^t \equiv 1$, dans le cas d'un module quelconque... 90
Des indices 91
Usage des indices dans la résolution des congruences binômes ... 93
Démonstration d'un théorème de Lagrange 94
Théorème de Legendre sur la loi de réciprocité qui existe entre deux nombres premiers 102
De la congruence $x^2 - N \equiv 0$ (mod. p), p étant un nombre premier 112
De la congruence $x^2 - N \equiv 0$, dans le cas d'un module quelconque. 117

CHAPITRE III.

PROPRIÉTÉS DES FONCTIONS ENTIÈRES D'UNE VARIABLE, RELATIVEMENT A UN MODULE PREMIER.

Des fonctions entières irréductibles suivant un module premier... 122
Remarques sur la decomposition d'une fonction entière en facteurs irréductibles 126
Des fonctions entières d'une variable, réduites suivant un module premier et suivant une fonction entière irréductible 129
Propriétés fondamentales des polynômes irréductibles suivant un module premier 132
Détermination du nombre des fonctions entières de degré ν irréductibles suivant un module premier p 137
Sur la décomposition d'une fonction entière donnée en facteurs irréductibles suivant un module premier 142
Classification des fonctions entières de degré ν irréductibles suivant le module premier p 144
Comparaison des fonctions entières irreductibles suivant le module p

Pages

qui appartiennent à des exposants formés des mêmes facteurs premiers 149

Sur une fonction irréductible du degré p suivant le module p..... 163

Classification des fonctions réduites suivant un module premier et suivant une fonction irréductible........ 164

Des congruences suivant un module premier et suivant une fonction modulaire........ 171

Propriétés des racines d'une congruence dont le premier membre est une fonction irréductible de degré égal au degré de la fonction modulaire ou égal à un sous-multiple de ce degré......... 174

Des racines primitives de la congruence

$$X^{p^{\nu}-1} - 1 \equiv 0 \; [\text{mod.}\, p,\; F(x)]$$ 175

Du point de vue sous lequel Galois a envisagé les congruences suivant un module premier et une fonction modulaire............ 179

Application de la théorie précédente au cas du module 7......... 181

CHAPITRE IV.

DÉTERMINATION DES FONCTIONS ENTIÈRES IRRÉDUCTIBLES, SUIVANT UN MODULE PREMIER, DANS LE CAS OU LE DEGRÉ EST UNE PUISSANCE DU MODULE.

Sur les fonctions entières irréductibles, suivant un module premier, dans le cas où le degré est égal au module.............. 190

Sur les fonctions entières irréductibles suivant un module premier, dans le cas où le degré est une puissance du module........... 195

CHAPITRE V.

SUR LA TOTALITÉ DES NOMBRES PREMIERS COMPRIS ENTRE DES LIMITES DONNÉES.

Sur l'évaluation approchée du produit $1.2.3\ldots x$, quand x est un grand nombre........ 212

Extension des formules précédentes au cas où x n'est pas un nombre entier positif........ 219

Détermination de deux limites entre lesquelles reste comprise la somme des logarithmes népériens de tous les entiers qui ne surpassent pas un nombre donné........ 225

Sur la totalité des nombres premiers compris entre deux limites données........ 226

Propriété fondamentale de la fonction $\theta(z)$.................... 227

Pages

Démonstration de deux inégalités auxquelles satisfait la fonction $\psi(z)$ 229
Détermination de deux limites entre lesquelles sont comprises les fonctions $\psi(z)$ et $\theta(z)$ 231
Détermination de deux limites du nombre qui indique combien il y a de nombres premiers compris entre deux nombres donnés... 236
Application des résultats qui précèdent 238

SECTION IV.

LES SUBSTITUTIONS.

CHAPITRE PREMIER.

PROPRIÉTÉS GÉNÉRALES DES SUBSTITUTIONS.

Des permutations formées avec des lettres données, et des substitutions par lesquelles on passe d'une permutation à une autre... 243
Des produits de substitutions........ 245
Ordre d'une substitution........ 247
Des substitutions circulaires........ 249
Décomposition d'une substitution quelconque en cycles........ 250
Décomposition d'une substitution donnée en facteurs primitifs... 254
Des substitutions semblables........ 257
Du nombre des substitutions semblables à une substitution donnée. 259
Des substitutions échangeables entre elles........ 260
Réduction d'une substitution quelconque à un produit de transpositions........ 273

CHAPITRE II.

PROPRIÉTÉS DES SYSTÈMES DE SUBSTITUTIONS CONJUGUÉES.

Des systèmes conjugués........ 278
Des systèmes semblables et des systèmes échangeables entre eux... 282
Du problème général qui fait l'objet principal de la théorie des substitutions........ 283
Des groupes de permutations........ 309

CHAPITRE III.

DES INDICES DES SYSTÈMES CONJUGUÉS.

Pages

Indice d'un système conjugué. — Limite inférieure des indices supérieurs à 2 314
Démonstration nouvelle du théorème relatif à la limite inférieure des indices plus grands que 2 324
Du système conjugué d'indice 6 qui comprend 120 substitutions de six lettres et qui n'est pas formé par les 120 substitutions de cinq lettres 335
Des systèmes transitifs de substitutions conjuguées 340
Des expressions susceptibles de représenter l'indice d'un système intransitif 349
Sur la limite des indices supérieurs à 2, dans le cas des systèmes transitifs 353

CHAPITRE IV.

SUR QUELQUES CAS PARTICULIERS DE LA THÉORIE DES SUBSTITUTIONS.

Sur les fonctions linéaires de la forme $\frac{ax+b}{a'x+b'}$ 356
Des fonctions rationnelles linéaires prises suivant un module premier 363
Des fonctions analytiques propres à représenter les substitutions... 383
Des substitutions rationnelles et linéaires 390
De quelques propriétés des substitutions linéaires 393
Sur les substitutions de cinq et de sept lettres 405

CHAPITRE V.

APPLICATIONS DE LA THÉORIE DES SUBSTITUTIONS.

Des valeurs diverses que prend une fonction de plusieurs variables par les substitutions de ces variables 413
Des fonctions semblables 417
Sur la formation des fonctions de n variables qui admettent des substitutions données 423
Des fonctions doublement transitives de n variables qui ont $1.2.3\ldots(n-2)$ valeurs, n étant premier 424
Des fonctions triplement transitives de $n+1$ variables qui ont $1.2.3\ldots(n-2)$ valeurs, n étant premier 428

Pages

Sur les fonctions triplement transitives de six variables qui ont six valeurs distinctes 432
Méthode de Lagrange pour calculer une fonction des racines d'une équation donnée quand on connaît une autre fonction quelconque des racines 433
Recherches de Galois relatives à la théorie précédente 441

SECTION V.

LA RÉSOLUTION ALGEBRIQUE DES ÉQUATIONS.

CHAPITRE PREMIER.

DES ÉQUATIONS DU TROISIÈME ET DU QUATRIÈME DEGRÉ. CONSIDÉRATIONS GÉNÉRALES SUR LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS.

Résolution de l'équation générale du troisième degré 451
Des équations du troisième degré dont deux racines peuvent s'exprimer rationnellement en fonction de la troisième racine et des quantités connues 466
Résolution de l'équation générale du quatrième degré 471
Sur la résolution algébrique des équations 482
Des équations dont le degré est un nombre premier 484
Des équations dont le degré est un nombre composé 491

CHAPITRE II.

DE L'IMPOSSIBILITÉ DE LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS GÉNÉRALES AU DELA DU QUATRIÈME DEGRÉ.

Des fonctions algébriques 497
Des fonctions entières 498
Des fonctions rationnelles 499
Classification des fonctions algébriques non rationnelles 500
Forme générale des fonctions algébriques 502
Propriété des fonctions algébriques qui satisfont à une équation donnée 506
Démonstration de l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième 512

CHAPITRE III.

DES ÉQUATIONS ABÉLIENNES.

Pages.

Des équations irréductibles dont deux racines sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre........ 518

Résolution algébrique des équations dont toutes les racines peuvent être représentées par θx, $\theta^2 x$, ..., $\theta^{\mu-1} x$, θx étant une fonction rationnelle de x et des quantités connues, telles que $\theta^{\mu} x = x$... 529

Cas où les quantités connues sont réelles........ 534

Première méthode particulière relative aux équations abéliennes dont le degré est un nombre composé........ 537

Deuxième méthode........ 542

Des équations irréductibles dont deux racines x et x' sont liées par la relation linéaire $x' = \frac{ax+b}{a'x+b'}$, où a, b, a', b' sont des constantes données........ 544

Des équations irréductibles à coefficients numériques dont plusieurs racines se développent en des fractions continues terminées par les mêmes quotients........ 546

Des équations dont toutes les racines sont exprimables rationnellement par l'une d'entre elles........ 552

Résolution algébrique des équations binômes........ 556

Résolution algébrique des équations dont dépend la division de la circonférence du cercle en un nombre premier de parties égales. 558

Division de la circonférence en dix-sept parties égales........ 565

Construction géométrique........ 569

Sur une propriété remarquable de la fonction $\frac{x^p - 1}{x - 1}$, p étant un nombre premier........ 573

Sur quelques propriétés de la fonction résolvante qui se rapporte à l'équation $\frac{x^p - 1}{x - 1} = 0$........ 582

Démonstration nouvelle de la loi de réciprocité de Legendre..... 590

CHAPITRE IV.

SUR UNE CLASSE D'ÉQUATIONS DU NEUVIÈME DEGRÉ RÉSOLUBLES ALGÉBRIQUEMENT.

Du déterminant d'une fonction entière et homogène de trois variables........ 594

Sur les points d'inflexion des courbes du troisième degré........ 601

Pages.
Sur un théorème de Steiner relatif aux courbes du troisième degré. 621
Propriété de l'équation du neuvième degré qui a pour racines les abscisses des points d'inflexion d'une courbe du troisième degré. 626
Sur la résolution algébrique d'une classe d'équations du neuvième degré 630

CHAPITRE V.

SUR LES ÉQUATIONS RÉSOLUBLES ALGÉBRIQUEMENT.

Recherches de Galois. — Théorèmes généraux 637
Suite des recherches de Galois. — Applications aux équations irréductibles de degré premier 664
Recherches de M. Hermite.................................... 677
Recherches de M. Kronecker.............. 684

FIN DE LA TABLE DES MATIÈRES DU TOME SECOND.

COURS
D'ALGÈBRE SUPÉRIEURE.

Les propriétés générales des équations et les questions d'Analyse qui s'y rattachent ont été développées dans le tome Ier de cet Ouvrage; il nous reste à traiter de la *résolution algébrique* des équations.

Mais, bien que cette importante question soit l'objet principal que nous ayons en vue, nous devons exposer d'abord les théories partielles dont nous aurons ensuite à emprunter le secours. Ces théories offrent d'ailleurs un grand intérêt par elles-mêmes; aussi les avons-nous présentées avec des développements étendus.

SECTION III.

LES PROPRIÉTÉS DES NOMBRES ENTIERS.

SECTION III.

LES PROPRIÉTÉS DES NOMBRES ENTIERS.

CHAPITRE PREMIER.

DES CONGRUENCES.

Des nombres congrus ou équivalents.

281. Si la différence des deux nombres entiers a et b, positifs ou négatifs, est divisible par un troisième nombre positif M, a et b sont dits *congrus* ou *équivalents* par rapport à M; le diviseur M est appelé le *module; a* et b sont *résidus l'un de l'autre* suivant le module M.

Pour exprimer que a et b sont congrus suivant le module M, il suffit d'écrire

$$a = b \pm \text{un multiple de M};$$

mais nous adopterons la notation plus commode de Gauss, et nous écrirons

$$a \equiv b \pmod{\text{M}};$$

cette formule sera dite une *congruence*.

Si r désigne le reste de la division de a par M, on a

$$a \equiv r \pmod{\text{M}};$$

le reste r est, si l'on veut, compris entre o et M, ou entre $-\frac{\text{M}}{2}$ et $+\frac{\text{M}}{2}$, d'où il suit que tout nombre a un résidu inférieur en valeur absolue à la moitié du module.

On le nomme *résidu minimum;* mais, si l'on ne veut considérer que les résidus positifs, les limites seront o et M, et le résidu minimum pourra surpasser $\frac{M}{2}$.

282. La notation de Gauss, pour représenter les congruences, a l'avantage de mettre en évidence l'analogie qui existe entre les congruences et les égalités, sans qu'il y ait pourtant de confusion à craindre. Nous allons faire voir que la plupart des transformations que l'on peut faire subir aux égalités peuvent être appliquées aux congruences.

Addition et soustraction. — Si l'on a

$$a \equiv b \pmod{M},$$
$$a' \equiv b' \pmod{M},$$

on aura aussi

$$a \pm a' \equiv b \pm b' \pmod{M}.$$

Les congruences proposées expriment, en effet, que

$$a = b + \text{un multiple de M},$$
$$a' = b' + \text{un multiple de M};$$

donc

$$a \pm a' = b \pm b' + \text{un multiple de M},$$

ou

$$a \pm a' \equiv b \pm b' \pmod{M},$$

ce qu'il fallait démontrer.

Multiplication. — On peut multiplier une congruence par un nombre entier quelconque; car soit

$$a \equiv b \pmod{M},$$

c'est-à-dire

$$a = b + \text{un multiple de M},$$

on aura aussi, quel que soit l'entier m,

$$ma = mb + \text{un multiple de M},$$

ou

$$ma \equiv mb \pmod{M}.$$

On peut aussi multiplier entre elles plusieurs congruences de même module. Soient, en effet, deux congruences

$$a \equiv b \pmod{M},$$
$$a' \equiv b' \pmod{M},$$

ou

$$a = b + \text{un multiple de } M,$$
$$a' = b' + \text{un multiple de } M.$$

On aura, en multipliant,

$$aa' = bb' + \text{un multiple de } M,$$

ou

$$aa' \equiv bb' \pmod{M},$$

ce qu'il fallait démontrer.

On voit généralement que, si l'on a

$$\left.\begin{array}{l} a \equiv b \\ a' \equiv b' \\ \ldots\ldots, \\ a^{(m)} \equiv b^{(m)} \end{array}\right\} \pmod{M},$$

on aura aussi

$$aa' \ldots a^{(m)} \equiv bb' \ldots b^{(m)} \pmod{M}.$$

Élévation aux puissances — On peut élever à une même puissance les deux membres d'une congruence. Cela résulte immédiatement de ce que nous venons de dire au sujet de la multiplication. Si donc on a

$$a \equiv b \pmod{M},$$

on aura aussi

$$a^m \equiv b^m \pmod{M}.$$

D'après cela, si

$$f(x) = Ax^m + Bx^n + \ldots$$

est une fonction entière et rationnelle de x, dont les coefficients A, B, ... soient des nombres entiers, et que l'on ait

$$a \equiv b \pmod{M},$$

on aura aussi

$$f(a) \equiv f(b) \pmod{M}.$$

Division. — On peut diviser une congruence par un nombre quelconque premier avec le module.

Soit, en effet, la congruence

$$ma \equiv mb \pmod{M}$$

ou

$$ma = mb + M \times q,$$

on aura, en divisant par m,

$$a = b + \frac{M \times q}{m},$$

et, si l'on suppose m premier avec M, q devra être divisible par m, et l'on aura

$$a = b + \text{un multiple de M},$$

ou

$$a \equiv b \pmod{M}.$$

Mais ce résultat ne subsiste pas quand le nombre m et le module M ont un diviseur commun; car soit $\frac{M'}{m'}$ la fraction irréductible équivalente à $\frac{M}{m}$, on aura

$$a = b + \frac{M' \times q}{m'};$$

cela exige seulement que q soit divisible par m', et l'on aura

$$a \equiv b \pmod{M'}.$$

On peut aussi diviser une congruence par une autre, pourvu que les membres de la seconde soient premiers

avec le module. Soient, en effet, les deux congruences

(1) $$aa' \equiv bb' \pmod{M},$$

(2) $$a \equiv b \pmod{M}.$$

Désignons par r le résidu minimum de la différence $a' - b'$, on aura

(3) $$a' \equiv b' \pm r \pmod{M},$$

et, en multipliant les congruences (2) et (3) l'une par l'autre,

(4) $$aa' \equiv bb' \pm br \pmod{M}.$$

Des congruences (1) et (4) on déduit

$$br \equiv 0 \pmod{M}:$$

or M est premier avec b, par hypothèse; donc

$$r \equiv 0 \pmod{M},$$

ou

$$r = 0,$$

puisque $r > M$. On a par conséquent

$$a' \equiv b' \pmod{M},$$

ce qu'il fallait démontrer.

Du nombre qui exprime combien il y a de nombres premiers à un nombre donné et non supérieurs à ce nombre.

283. Lemme. — *Si l'on multiplie les termes de la suite*

(1) $$1,\ 2,\ 3,\ \ldots,\ (M-1)$$

par un entier a premier avec M, *les produits obtenus*

(2) $$a,\ 2a,\ 3a,\ \ldots,\ (M-1)a$$

seront respectivement congrus, suivant le module M, *aux nombres* (1), *abstraction faite de l'ordre.*

En effet, l'un des nombres (2), ma par exemple, ne saurait être divisible par M, puisque M est premier avec a et qu'il est supérieur à m; la même chose a lieu, à l'égard de la différence $ma - m'a$ de deux termes de la suite (2), car cette différence est aussi un terme de la même suite. Il résulte de là que, si l'on prend les résidus minima positifs des nombres (1), par rapport à M, ces résidus seront tous différents et aucun d'eux ne sera nul; ce seront donc, dans un certain ordre, les nombres de la suite (1).

Corollaire. — *Si le nombre* M *est premier à* a, *les termes de la progression arithmétique*

(1) $$c,\ c+a,\ c+2a,\ \ldots\ c+(M-1)a,$$

sont respectivement congrus, suivant le module M, *quel que soit l'entier* c, *aux nombres*

(2) $$0,\ 1,\ 2,\ \ldots,\ (M-1).$$

En effet, d'après le lemme précédent, les nombres (1) sont respectivement congrus à

$$c,\ c+1,\ c+2,\ \ldots,\ c+(M-1),$$

et il est évident que ces derniers sont congrus aux nombres (2), suivant le module M.

284. Nous emploierons le symbole $\varphi(M)$ pour désigner combien il y a de nombres premiers à M et *non supérieurs* à M. D'après cette définition, on a évidemment

$$\varphi(1) = 1.$$

Théorème. — *Si* M *désigne le produit de plusieurs nombres* a, b, ..., l, *premiers entre eux deux à deux, on aura*

$$\varphi(M) = \varphi(a)\,\varphi(b)\ldots\varphi(l).$$

Prenons d'abord le cas de deux facteurs et soit

$$M = ab,$$

a et b désignant des nombres premiers entre eux. Les ab premiers nombres peuvent être disposés comme il suit :

$$\begin{array}{llll} 1, & 2, \ldots, & k, \ldots, & b, \\ b+1, & b+2, \ldots, & b+k, \ldots, & b+b, \\ 2b+1, & 2b+2, \ldots, & 2b+k, \ldots, & 2b+b, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots, \\ (a-1)b+1, & (a-1)b+2, \ldots, & (a-1)b+k, \ldots, & (a-1)b+b. \end{array}$$

Considérons l'une des colonnes verticales de ce tableau, par exemple celle qui commence par k. Si k est premier avec b, il en sera de même de tous les autres termes de la colonne ; au contraire, si k et b ont un diviseur commun autre que 1, il n'y aura dans la colonne aucun nombre premier avec b. D'ailleurs, la première ligne du tableau renferme $\varphi(b)$ nombres premiers avec b ; donc le tableau entier renferme $\varphi(b)$ colonnes verticales dont tous les termes sont premiers à b, et qui épuisent tous les nombres de cette espèce non supérieurs à M. Supposons que k soit premier avec b ; la colonne verticale qui commence par k est une progression arithmétique dont les termes sont respectivement congrus, suivant le module a, aux nombres $0, 1, 2, \ldots, (a-1)$; cette dernière suite contient $\varphi(a)$ nombres premiers à a, et, par conséquent, la colonne que nous considérons en renferme un pareil nombre. De tout cela il résulte que notre tableau renferme $\varphi(a) \times \varphi(b)$ nombres premiers à a et à b, c'est-à-dire premiers au produit ab ; on a donc

$$\varphi(M) = \varphi(a)\varphi(b).$$

Passons maintenant au cas général où l'on a

$$M = abc\ldots l,$$

a, b, c,..., l étant des nombres premiers entre eux, deux à deux. On aura successivement

$$\begin{aligned}\varphi(M) &= \varphi(a)\varphi(b.c\ldots l)\\ &= \varphi(a)\varphi(b)\varphi(c\ldots l)\\ &= \varphi(a)\varphi(b)\varphi(c)\varphi(\ldots l)\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ &= \varphi(a)\varphi(b)\varphi(c)\ldots\varphi(l),\end{aligned}$$

ce qui achève la démonstration du théorème énoncé.

285. Le théorème précédent fournit un moyen très-simple de trouver la valeur de $\varphi(M)$.

Lorsque M est égal à un nombre premier p, il est évident que les nombres premiers à $M = p$, et non supérieurs à ce nombre, sont

$$1, 2, 3, \ldots, (p-1);$$

on a donc

$$\varphi(p) = p - 1.$$

Lorsque M est égal à une puissance p^ν d'un nombre premier p, il est évident que la suite des $p^{\nu-1}$ nombres

$$p, 2p, 3p, \ldots, p^{\nu-1}.p$$

renferme tous les nombres non supérieurs à M qui admettent p pour diviseur; on a donc

$$\varphi(M) = p^\nu - p^{\nu-1} = p^{\nu-1}(p-1),$$

ou

$$\varphi(M) = M\left(1 - \frac{1}{p}\right).$$

Considérons le cas général; soient p, q, r, ... les facteurs premiers inégaux de M, et supposons

$$M = p^\nu q^\mu r^\lambda \ldots,$$

$\nu, \mu, \lambda, \ldots$ étant des exposants entiers. On aura (n° 284)

$$\varphi(M) = \varphi(p^\nu)\,\varphi(q^\mu)\,\varphi(r^\lambda)\ldots;$$

d'ailleurs

$$\varphi(p^\nu) = p^\nu\left(1 - \frac{1}{p}\right),$$

$$\varphi(q^\mu) = q^\mu\left(1 - \frac{1}{q}\right),$$

$$\varphi(r^\lambda) = r^\lambda\left(1 - \frac{1}{r}\right)\ldots;$$

donc

$$\varphi(M) = p^\nu q^\mu r^\lambda \ldots \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\ldots,$$

ou

$$\varphi(M) = M\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\ldots.$$

Il importe de remarquer que, si M est un nombre impair, on a

$$\varphi(2M) = \varphi(2)\,\varphi(M);$$

or $\varphi(2) = 1$: donc

$$\varphi(2M) = \varphi(M).$$

286. Il convient de remarquer encore le théorème suivant, qui nous sera très-utile dans la suite :

Théorème. — *Si* $d, d', d'', \ldots$ *désignent la suite des diviseurs du nombre* M, *parmi lesquels figurent l'unité et le nombre* M *lui-même, on a*

$$\varphi(d) + \varphi(d') + \varphi(d'') + \ldots = M.$$

En effet, soit

$$M = p^\nu q^\mu r^\lambda \ldots,$$

$p, q, r, \ldots$ étant des nombres premiers inégaux ; les diviseurs $d, d', d'', \ldots$ ne seront autre chose que les

termes du polynôme égal au produit

$$(1+p+p^2+\ldots+p^\nu)(1+q+q^2+\ldots+q^\mu)(1+r+\ldots+r^\lambda)\ldots.$$

L'un quelconque des termes du polynôme dont il s'agit a la forme $p^\alpha q^\beta r^\gamma\ldots$; d'ailleurs l'égalité

$$d=p^\alpha q^\beta r^\gamma\ldots$$

entraîne

$$\varphi(d)=\varphi(p^\alpha)\varphi(q^\beta)\varphi(r^\gamma)\ldots;$$

donc la somme de toutes les quantités $\varphi(d)$ sera le produit des polynômes

$$\begin{array}{l} 1+\varphi(p)+\varphi(p^2)+\ldots+\varphi(p^\nu),\\ 1+\varphi(q)+\varphi(q^2)+\ldots+\varphi(q^\mu),\\ 1+\varphi(r)+\varphi(r^2)+\ldots+\varphi(r^\lambda),\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}$$

Le premier de ces polynômes a pour valeur

$$1+(p-1)(1+p+p^2+\ldots+p^{\nu-1})=p^\nu,$$

et l'on voit de même que les polynômes suivants ont respectivement pour valeurs q^μ, r^λ, ...; on a donc

$$\varphi(d)+\varphi(d')+\varphi(d'')+\ldots=p^\nu q^\mu r^\lambda\ldots=\mathrm{M}.$$

Des congruences en général.

287. La théorie des nombres résout sur les congruences le même problème que l'Algèbre ordinaire sur les équations; elle se propose, en particulier, de trouver les valeurs de x qui satisfont à une congruence telle que

$$f(x)\equiv 0 \pmod{\mathrm{M}},$$

où $f(x)$ désigne un polynôme entier et rationnel dont les coefficients sont des nombres entiers. Si l'on satis-

fait à cette congruence, en faisant $x = a$, on y satisfera aussi, d'après une remarque précédente, en faisant, quel que soit l'entier k, $x = a + kM$; d'où il suit que chaque solution en donne une infinité d'autres, mais qui sont toutes équivalentes suivant le module M. Les diverses solutions renfermées dans une même formule $a + kM$ peuvent se déduire de l'une quelconque d'entre elles; d'ailleurs, on peut disposer de l'entier k de manière que $a + kM$ soit compris entre $-\frac{M}{2}$ et $+\frac{M}{2}$, ou entre o et M; il n'y a donc lieu de s'occuper que des solutions comprises entre ces limites.

Cela posé, nous appellerons *racines* de la congruence

$$f(x) \equiv 0 \pmod{M}$$

les diverses valeurs de x comprises entre o et M, qui rendent $f(x)$ divisible par M.

Une congruence est *identique* lorsque tous ses coefficients sont divisibles par le module, et elle est évidemment impossible lorsque ses coefficients sont divisibles par l'un des facteurs du module, à l'exception du terme indépendant de x.

Si $F(x)$ désigne un polynôme entier et rationnel, ayant pour coefficients des nombres entiers, on peut substituer à la congruence

$$f(x) \equiv 0 \pmod{M}$$

la congruence équivalente

$$f(x) + MF(x) \equiv 0 \pmod{M},$$

et disposer ensuite des coefficients indéterminés de $F(x)$, pour rabaisser au-dessous de M, et même de $\frac{M}{2}$ si l'on veut, tous les coefficients de la congruence.

Des congruences du premier degré.

288. La congruence du premier degré

$$(1) \qquad ax + b \equiv 0 \pmod{M}$$

peut se mettre sous la forme

$$(2) \qquad ax + b = My,$$

et la recherche de ses racines est ramenée à celle des solutions en nombres entiers de l'équation (2) qui renferme les deux inconnues x et y. Si a et M sont premiers entre eux, l'équation (2) est toujours résoluble en nombres entiers; on obtient une première solution x_0, y_0 (n° 13) par la réduction de $\frac{a}{M}$ en fraction continue; après quoi toutes les solutions sont données par les formules

$$x = x_0 + Mt, \quad y = y_0 + at,$$

où t désigne une indéterminée. On peut disposer de cette indéterminée de manière à obtenir une valeur de x comprise entre zéro et M, et, si l'on représente cette valeur par x_0, les autres valeurs de x continueront à être données par la première des formules qui précèdent.

Il résulte de là que la congruence du premier degré (1) n'admet qu'une seule racine, quel que soit le module, lorsque le coefficient de l'inconnue est premier avec ce module.

On arrive à la même conclusion au moyen du lemme du n° 283 (Corollaire). Effectivement, si l'on donne à x les M valeurs

$$0, \ 1, \ 2, \ \ldots, \ (M-1),$$

le premier membre de la congruence (1) prendra M valeurs incongrues suivant le module M; l'une de ces

valeurs sera donc nulle, relativement à ce module, et la valeur correspondante de x sera la racine demandée.

Si x_0 désigne cette racine, on peut écrire

$$x_0 \equiv -\frac{b}{a} \quad (\text{mod. M}),$$

comme Gauss l'a proposé.

Si le coefficient a n'est pas premier avec le module M et que d désigne le plus grand commun diviseur de ces deux nombres, la congruence (1) ne sera résoluble que si b est divisible par d. Quand il en est ainsi, la congruence, divisée par d, devient

$$(3) \qquad \frac{a}{d}x + \frac{b}{d} \equiv 0 \quad \left(\text{mod. } \frac{M}{d}\right);$$

on rentre alors dans le cas que nous venons d'examiner. Soit x_0 la racine de la congruence (3) : les valeurs de x qui pourront y satisfaire seront toutes comprises dans la formule

$$x = x_0 + \frac{M}{d}t,$$

et l'on voit que la proposée admettra les d racines

$$x_0, \; x_0 + \frac{M}{d}, \; x_0 + \frac{2M}{d}, \; \ldots, \; x_0 + \frac{(d-1)M}{d},$$

qui sont incongrues suivant le module M.

289. Lorsque le module M est un nombre composé, la résolution de la congruence

$$(1) \qquad ax + b \equiv 0 \quad (\text{mod. M}),$$

où l'on suppose a premier avec M, peut être ramenée à celle d'autres congruences dans chacune desquelles le module est un facteur de M.

Soit, en effet,

$$M = M_1 M_2,$$

M_1 et M_2 étant des nombres entiers.

Il est évident que la racine de la congruence (1) doit satisfaire à la congruence

$$(2) \qquad ax + b \equiv 0 \pmod{M_1};$$

désignons par α la racine de cette congruence : les valeurs de x qui satisfont à la proposée seront de la forme

$$x = \alpha + M_1 x_1.$$

x_1 étant une indéterminée, et en substituant cette valeur il viendra

$$(a\alpha + b) + M_1 a x_1 \equiv 0 \pmod{M}.$$

Par hypothèse, $a\alpha + b$ est divisible par M_1; si donc on pose

$$\frac{a\alpha + b}{M_1} = b_1,$$

la précédente congruence, divisée par M_1, deviendra

$$ax_1 + b_1 \equiv 0 \pmod{M_2}.$$

Si l'on désigne par α_1 la racine de cette nouvelle congruence, la formule

$$x = \alpha + M_1 \alpha_1$$

donnera la racine de la proposée.

On conclut de là que, si l'on a

$$M = M_1 M_2 \ldots M_k,$$

$M_1, M_2, \ldots, M_k$ étant des nombres entiers, la résolution de la congruence

$$ax + b \equiv 0 \pmod{M}$$

peut être ramenée à celle d'autres congruences de la forme

$$ax + b \equiv 0 \pmod{M_1},$$
$$ax + b_1 \equiv 0 \pmod{M_2},$$
$$\dots\dots\dots\dots\dots\dots\dots,$$
$$ax + b_{k-1} \equiv 0 \pmod{M_k}.$$

En particulier, on peut prendre pour les nombres M_1, M_2, ... les facteurs premiers dont le module est le produit.

Exemple. — Soit la congruence

$$1237x - 4096 \equiv 0 \pmod{675}.$$

Le module 675 est égal au produit 27×25; on peut donc commencer par résoudre la congruence

$$1237x - 4096 \equiv 0 \pmod{27},$$

qui, en rabaissant les coefficients au-dessous du module, devient

$$5x - 8 \equiv 0 \pmod{27},$$

ou, si l'on veut,

$$x = \frac{8 + 27y}{5}.$$

La valeur $y = 1$ donne $x = 7$; on fera, en conséquence,

$$x = 7 + 27x_1;$$

en substituant cette valeur, la proposée devient

$$1237 \times 27x_1 + 4563 \equiv 0 \pmod{27 \times 25},$$

ou, en divisant par 27,

$$1237x_1 + 169 \equiv 0 \pmod{25};$$

rabaissant les coefficients au-dessous du module 25, on obtient

$$12x_1 - 6 \equiv 0 \pmod{25},$$

ou, en divisant par 6, qui est premier avec le module,

$$2x_1 - 1 \equiv 0 \pmod{25}.$$

On tire de là

$$x_1 = \frac{1 + 25y}{2},$$

et la valeur $y = 1$ donne $x_1 = 13$.

La racine demandée est donc

$$x = 7 + 27 \times 13 = 358.$$

290. On ramène au problème dont nous venons de nous occuper celui qui a pour objet de trouver un nombre N qui ait des résidus donnés $a, a_1, a_2, \ldots,$ suivant des modules donnés $M, M_1, M_2, \ldots.$

Le nombre cherché N doit satisfaire aux congruences

$$(1)\quad N \equiv a \pmod{M},\quad N \equiv a_1 \pmod{M_1},\quad N \equiv a_2 \pmod{M_2}, \ldots:$$

la première donne

$$N = a + Mx,$$

et, pour que le nombre N ainsi déterminé satisfasse aussi à la deuxième des congruences (1), il faut que l'on ait

$$a + Mx \equiv a_1 \pmod{M_1} \quad \text{ou} \quad Mx + (a - a_1) \equiv 0 \pmod{M_1}.$$

Si le plus grand commun diviseur d des nombres M et M_1 ne divise pas $a - a_1$, le problème proposé n'admettra pas de solution; dans le cas contraire, la précédente congruence peut s'écrire

$$\frac{M}{d}x + \frac{a - a_1}{d} \equiv 0 \quad \left(\text{mod.}\ \frac{M_1}{d}\right),$$

et, si l'on désigne par α sa racine, cette congruence ne sera satisfaite que par les valeurs de x données par la

formule

$$x = \alpha + \frac{M_1}{d} x_1,$$

x_1 étant une indéterminée. En posant

$$a + M\alpha = a^{(1)},$$

on obtient cette expression de N

$$N = a^{(1)} + \frac{MM_1}{d} x_1.$$

Si l'on veut que cette valeur de N satisfasse à la troisième des congruences (1), il faudra que l'on ait

$$a^{(1)} + \frac{MM_1}{d} x_1 \equiv a_2 \pmod{M_2},$$

ou

$$\frac{MM_1}{d} x_1 + (a^{(1)} - a_2) \equiv 0 \pmod{M_2};$$

si le plus grand commun diviseur d_1 des nombres $\frac{MM_1}{d}$ et M_2 ne divise pas $a^{(1)} - a_2$, la précédente congruence sera impossible; dans le cas contraire, elle se ramènera à la forme

$$\frac{MM_1}{dd_1} x_1 + \frac{a^{(1)} - a_2}{d_1} \equiv 0 \quad \left(\text{mod. } \frac{M_2}{d_1}\right),$$

et, en appelant α_1 sa racine, on devra poser

$$x_1 = \alpha_1 + \frac{M_2}{d_1} x_2,$$

x_2 étant une indéterminée. Faisant alors

$$a^{(1)} + \frac{MM_1}{d} \alpha_1 = a^{(2)},$$

l'expression de N sera

$$N = a^{(2)} + \frac{MM_1M_2}{dd_1} x_2.$$

On peut continuer de cette manière jusqu'à ce qu'on ait épuisé toutes les congruences proposées, et si l'on ne rencontre aucune congruence impossible, l'expression demandée aura la forme

$$N = A + \mu X,$$

X étant une indéterminée, et μ désignant le plus petit commun multiple des modules M, M_1, M_2, ...

291. Le cas d'un nombre m de congruences du premier degré, à m indéterminées, peut être résolu au moyen de ce qui précède. Supposons qu'on demande les systèmes de solutions des congruences

$$(1)\quad \left.\begin{cases} a_0 x + b_0 y + c_0 z + \ldots + k_0 u + l_0 \equiv 0 \\ a_1 x + b_1 y + c_1 z + \ldots + k_1 u + l_1 \equiv 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m-1} x + b_{m-1} y + c_{m-1} z + \ldots + k_{m-1} u + l_{m-1} \equiv 0 \end{cases}\right\} \pmod{M}.$$

Les valeurs de l'une quelconque des inconnues, qui figurent dans les systèmes de solutions cherchées, dépendent d'une congruence linéaire qu'on peut facilement former. Effectivement on peut toujours trouver, par la théorie des équations du premier degré, m nombres entiers $\xi_0, \xi_1, \ldots, \xi_{m-1}$ qui n'aient aucun diviseur commun avec le module et qui satisfassent aux $m - 1$ équations

$$(2)\quad \begin{cases} b_0 \xi_0 + b_1 \xi_1 + \ldots + b_{m-1} \xi_{m-1} = 0, \\ c_0 \xi_0 + c_1 \xi_1 + \ldots + c_{m-1} \xi_{m-1} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ k_0 \xi_0 + k_1 \xi_1 + \ldots + k_{m-1} \xi_{m-1} = 0; \end{cases}$$

alors, si l'on ajoute les congruences (1) après les avoir multipliées par $\xi_0, \xi_1, \ldots, \xi_{m-1}$ respectivement, et que l'on fasse, pour abréger,

$$a_0 \xi_0 + a_1 \xi_1 + \ldots + a_{m-1} \xi_{m-1} = a,$$
$$l_0 \xi_0 + l_1 \xi_1 + \ldots + l_{m-1} \xi_{m-1} = l,$$

on aura

$$ax + l \equiv 0 \pmod{M}.$$

On peut opérer de la même manière à l'égard des inconnues $y, z, \ldots$, et l'on formera ainsi m congruences, dont chacune ne contiendra qu'une seule inconnue et qui admettront toutes les solutions du système proposé. Mais la réciproque de cette proposition n'a pas lieu, et il pourra arriver que diverses solutions du système obtenu par notre méthode ne conviennent point au système proposé. Dans la pratique, il sera en général plus simple de procéder par éliminations successives et de remplacer le système (1) par un autre dans lequel chaque congruence renferme une inconnue de moins que la précédente.

Exemple. — Soient les congruences

$$(1) \qquad \left\{ \begin{array}{l} 3x + 5y + z \equiv 4 \\ 2x + 3y + 2z \equiv 7 \\ 5x + y + 3z \equiv 6 \end{array} \right\} \pmod{12},$$

que Gauss a choisies pour exemple dans ses *Recherches arithmétiques*. Si l'on tire de la première la valeur de z pour la porter dans les deux autres, on aura ce nouveau système :

$$(2) \qquad \left\{ \begin{array}{l} z \equiv 4 - 3x - 5y \\ 4x + 7y \equiv 1 \\ 4x + 2y \equiv 6 \end{array} \right\} \pmod{12};$$

éliminant ensuite x entre les deux dernières, on a ce

troisième système :

$$(3)\qquad \left\{\begin{array}{l} z \equiv 4 - 3x - 5y \\ 4x \equiv 1 - 7y \\ 5y \equiv -5 \end{array}\right\} \pmod{12}.$$

La dernière congruence du système (3) n'a qu'une seule racine, qui est -1 ou 11. La deuxième des congruences (3) donne ensuite

$$4x \equiv 8 \pmod{12}$$

ou

$$x \equiv 2 \pmod{3}.$$

On a ainsi quatre valeurs de x, savoir :

$$x = 2,\ 5,\ 8,\ 11.$$

La première congruence (3), qui se réduit à

$$z \equiv 9 - 3x,$$

à cause de $y = -1$, donne les quatre valeurs correspondantes de z, savoir

$$z = 3,\ 6,\ 9,\ 0.$$

Sur le nombre des racines de la congruence $x^2 - 1 \equiv 0 \pmod{M}$.

292. Pour que le produit $(x+1)(x-1)$ soit divisible par M, il faut et il suffit que $x-1$ contienne tous ceux des facteurs premiers de M qui ne figurent pas dans $x+1$; d'ailleurs $x-1$ et $x+1$ ne peuvent avoir que les diviseurs 1 et 2 communs, puisque leur différence est égale à 2. Donc, pour résoudre la congruence

$$(1)\qquad x^2 - 1 \equiv 0 \pmod{M},$$

il suffira de poser de toutes les manières possibles

$$M = AB,$$

A et B étant premiers entre eux, ou ayant 2 pour plus grand commun diviseur, puis de déterminer les valeurs de x qui satisfont à la fois aux deux congruences

$$(2)\qquad x+1\equiv 0 \pmod{A},\quad x-1\equiv 0 \pmod{B}.$$

On tire de la première

$$(3)\qquad x=-1+At,$$

t étant une indéterminée, et, en substituant cette valeur dans la seconde congruence, il vient

$$(4)\qquad At-2\equiv 0 \pmod{B}.$$

Comme le plus grand commun diviseur de A et B est 1 ou 2, par hypothèse, la congruence (4) sera toujours possible. Si A et B sont premiers entre eux, cette congruence aura une racine unique et la formule (3) donnera également pour x une valeur unique. Mais, si A et B ont le diviseur commun 2, la congruence (4), divisée par 2, deviendra

$$(5)\qquad \frac{A}{2}t-1\equiv 0 \left(\text{mod.}\ \frac{B}{2}\right).$$

Les valeurs de t qui satisfont à la congruence (5) sont données par la formule

$$t=t_0+\frac{B}{2}u,$$

t_0 étant un nombre déterminé compris entre o et $\frac{B}{2}$, et u désignant une nouvelle variable. Alors la congruence (4) a les deux racines

$$t_0,\quad t_0+\frac{B}{2},$$

et la formule (3) donne les valeurs correspondantes de x,

$$-1+At_0,\quad -1+At_0+\frac{M}{2}.$$

Il importe d'examiner maintenant si l'une des racines de la congruence proposée peut être donnée par deux décompositions distinctes du module M :

$$M = AB, \quad M = A'B'.$$

Désignons par $\frac{a}{b}$ la fraction irréductible équivalente aux deux fractions

$$\frac{A}{B'}, \quad \frac{A'}{B},$$

lesquelles sont égales, en vertu de l'hypothèse $AB = A'B'$; on aura

$$A = \lambda a, \quad A' = \mu a,$$
$$B' = \lambda b, \quad B = \mu b,$$

et, par suite,

$$A' = \frac{\mu}{\lambda} A, \quad B' = \frac{\lambda}{\mu} B,$$

λ et μ étant des entiers. Mais, si les décompositions considérées fournissent une même racine x de la congruence (1), les nombres A et B' ou A' et B diviseront respectivement $x + 1$ et $x - 1$: donc ils ont pour plus grand commun diviseur 1 ou 2; chacun des nombres λ et μ est par suite égal à 1 ou à 2. Il résulte de là que les décompositions

$$M = \frac{1}{2} A \times 2B, \quad M = 2A \times \frac{1}{2} B$$

sont les seules qui puissent donner une racine x déjà fournie par la décomposition $M = AB$.

Cela posé, il est facile de déterminer le nombre N des racines distinctes de la congruence (1).

Supposons d'abord que le module M soit impair et désignons par n le nombre de ses facteurs premiers inégaux. Dans le cas dont il s'agit, les décompositions $M = AB$

donnent nécessairement des racines distinctes, et il suffit d'avoir le nombre de ces décompositions. Or, pour former A, on peut n'employer aucun des facteurs premiers de M : on aura alors $A = 1$; on peut introduire dans A un seul des n facteurs premiers de M, et l'on obtiendra ainsi n décompositions distinctes ; pareillement, on aura $\frac{n(n-1)}{1.2}$ décompositions, en formant A avec deux des facteurs premiers de M, et ainsi de suite. D'après cela, on aura

$$N = 1 + \frac{n}{1} + \frac{n(n-1)}{1.2} + \ldots + \frac{n}{1} + 1$$

ou

$$N = 2^n.$$

Supposons en deuxième lieu que le module M soit double d'un nombre impair, et désignons par g, comme précédemment, le nombre des facteurs premiers impairs inégaux de M ou de $\frac{M}{2}$. Considérons la décomposition

$$M = AB,$$

A étant pair et B impair ; parmi les autres décompositions, la seule qui puisse fournir la même racine x que la première est

$$M = \frac{1}{2} A \times 2B,$$

et je dis qu'elle la fournit effectivement. En effet, la racine qui répond à la première décomposition est déterminée par les formules

$$x = -1 + At, \quad At - 2 \equiv 0 \pmod{B};$$

or, A étant pair et B impair, on peut écrire

$$x = -1 + \frac{A}{2} \cdot 2t, \quad \frac{A}{2} \cdot 2t - 2 \equiv 0 \pmod{2B},$$

ce qui montre que cette valeur de x répond aussi à la seconde décomposition. Il résulte de là que N est le nombre des décompositions de $\frac{M}{2}$ en deux facteurs premiers entre eux, et l'on aura alors

$$N = 2^n,$$

comme dans le premier cas.

Supposons, enfin, que M soit divisible par la puissance 2^ρ de 2, ρ étant > 1, et désignons encore par n le nombre des facteurs premiers impairs inégaux de M ou de $\frac{M}{2^\rho}$. Dans ce cas, on peut rejeter toute décomposition

$$M = AB,$$

dans laquelle l'un des nombres A ou B serait impair. En effet, supposons A pair et B impair; le raisonnement que nous venons de faire, à l'occasion du cas précédent, montre que la racine qui répond à la décomposition AB sera aussi donnée par la décomposition $\frac{A}{2} \times 2B$. Maintenant une décomposition de M en deux facteurs pairs donne deux racines x qui sont nécessairement distinctes de celles fournies par une autre décomposition de la même espèce; car, dans chaque décomposition, les facteurs doivent avoir 2 pour plus grand commun diviseur; donc, pour obtenir toutes les décompositions utiles de M, il faut former celles de $\frac{M}{2^\rho}$ et introduire ensuite 2 dans le premier facteur, $2^{\rho-1}$ dans le second, puis inversement $2^{\rho-1}$ dans le premier facteur et 2 dans le second. Si $\rho = 2$, ces deux dernières opérations rentreront évidemment l'une dans l'autre.

Il résulte de là que, si $\rho = 2$, c'est-à-dire si M est divi-

sible par 4, mais non par 8, on aura

$$N = 2^{n+1}.$$

Si ρ est > 2, c'est-à-dire si M est divisible par 8, on aura

$$N = 2^{n+2}.$$

Cette conclusion n'est point en défaut, quand on a $M = 2^\rho$; dans ce cas, $\frac{M}{2^\rho}$ n'admet que la seule décomposition 1×1.

Il faut remarquer que les racines de la congruence (2) sont *conjuguées* deux à deux, de manière que deux racines conjuguées soient égales et de signes contraires, ou, si l'on veut, complémentaires au module. Il est évident que deux racines conjuguées sont fournies par deux décompositions telles que AB, BA.

Corollaire. — *La congruence*

$$x^2 - 1 \equiv 0 \pmod{M}$$

admet un couple unique de racines conjuguées dans l'un des trois cas suivants ; 1° si M *est une puissance d'un nombre premier impair; 2° si* M *est le double d'une telle puissance; 3° si* M *est égal à* 4. *Dans tout autre cas le nombre des couples de racines conjuguées de la congruence est un nombre pair.*

Ce corollaire résulte immédiatement des formules par lesquelles nous avons exprimé le nombre N dans les différents cas que nous avons examinés.

Exemple. — Si l'on a $M = 24$, on a ces quatre décompositions utiles

$$A = 2,\ 12,\ 4,\ 6,$$
$$B = 12,\ 2,\ 6,\ 4;$$

la congruence

$$x^2 - 1 \equiv 0 \pmod{24}$$

a huit racines, savoir :

1,	13	fournies par la décomposition		2×12,
23,	11	»	»	12×2,
7,	19	»	»	4×6,
17,	5	»	»	6×4.

Théorème de Fermat.

293. Le théorème de Fermat est l'une des propositions fondamentales de la théorie qui nous occupe; aussi croyons-nous utile de présenter ici les démonstrations diverses qu'on en a données. Ce théorème célèbre est le suivant :

Théorème. — *Si le nombre entier a n'est pas divisible par le nombre premier p, la différence $a^{p-1}-1$ est divisible par p; en d'autres termes, on a*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Première démonstration. — Comme a et p sont premiers entre eux, par hypothèse, les nombres

$$(1) \qquad a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$$

donneront, relativement à p (n° 283), les résidus

$$(2) \qquad 1,\ 2,\ 3,\ \ldots.\ (p-1),$$

abstraction faite de l'ordre. Le produit des nombres (1) est donc congru, suivant le module p, au produit des nombres (2), et l'on a, en conséquence,

$$1.2.3\ldots(p-1)(a^{p-1}-1) \equiv 0 \pmod{p}.$$

On peut diviser cette congruence par le produit $1.2.3\ldots(p-1)$ qui est premier avec le module, et l'on a

$$a^{p-1}-1 \equiv 0 \pmod{p},$$

ce qu'il fallait démontrer.

Deuxième démonstration. — Si l'on élève à la puissance p le binôme

$$(a-1)+1,$$

dont la valeur est a, on aura

$$a^p = (a-1)^p + \frac{p}{1}(a-1)^{p-1} + \ldots$$
$$+ \frac{p(p-1)\ldots(p-k+1)}{1.2\ldots k}(a-1)^{p-k} + \ldots + 1;$$

dans le second membre de cette formule, tous les termes sont divisibles par p, à l'exception du premier et du dernier, car le coefficient

$$\frac{p(p-1)\ldots(p-k+1)}{1.2\ldots k}$$

est un nombre entier, et cet entier est évidemment divisible par p si k est $<p$. On a donc

$$a^p \equiv (a-1)^p + 1 \pmod{p},$$

et, en retranchant a, de part et d'autre,

$$a^p - a \equiv (a-1)^p - (a-1) \pmod{p}.$$

Cette formule montre que la différence $a^p - a$ n'est altérée que par un multiple de p, quand on diminue a d'une unité ; il en est donc de même quand on diminue a de 2, 3, ..., a unités ; on a, en conséquence,

$$a^p - a \equiv 0 \pmod{p},$$

et, en divisant par a, nombre premier au module, il vient

$$a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Troisième démonstration. — On a, quels que soient les entiers u et v,

$$(u+v)^p = u^p + \frac{p}{1}u^{p-1}v + \ldots$$
$$+ \frac{p(p-1)\ldots(p-k+1)}{1.2\ldots k}u^{p-k}v^k + \ldots + v^p;$$

nous avons vu que, dans le second membre de cette formule, tous les termes sont divisibles par p, à l'exception du premier et du dernier; on a donc

$$(u+v)^p \equiv u^p + v^p \pmod{p}.$$

Soient maintenant a nombres entiers $\alpha_1, \alpha_2, \ldots, \alpha_a$; on aura, d'après la formule précédente,

$$\left.\begin{array}{ll} (\alpha_1+\alpha_2+\ldots+\alpha_a)^p \equiv \alpha_1^p + (\alpha_2+\ldots+\alpha_a)^p \\ (\alpha_2+\alpha_3+\ldots+\alpha_a)^p \equiv \alpha_2^p + (\alpha_3+\ldots+\alpha_a)^p \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (\alpha_{a-1}+\alpha_a)^p \equiv \alpha_{a-1}^p + \alpha_a^p \end{array}\right\} \pmod{p},$$

et, en ajoutant,

$$(\alpha_1+\alpha_2+\ldots+\alpha_a)^p \equiv \alpha_1^p+\alpha_2^p+\ldots+\alpha_a^p \pmod{p}.$$

Supposons maintenant que les nombres $\alpha_1, \alpha_2, \ldots, \alpha_a$ se réduisent tous à l'unité, on aura

$$a^p \equiv a \pmod{p},$$

ou, en divisant par a,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Théorème de Wilson.

294. Théorème. — *Si p est un nombre premier, la somme $1.2.3\ldots(p-1)+1$ est divisible par p; en d'autres termes, on a*

$$1.2.3\ldots(p-1) \equiv -1 \pmod{p}.$$

Première démonstration. — Soit a l'un quelconque des nombres

(1) $$1,\ 2,\ 3,\ \ldots,\ (p-1),$$

et formons les multiples de a

(2) $a,\ 2a,\ 3a,\ \ldots,\ (p-1)a.$

Dans la suite (2), il y a un terme congru à 1, et il n'y en a qu'un seul; supposons que ce soit αa, on aura

$$\alpha a \equiv 1 \pmod{p}.$$

Les nombres a et α sont inégaux, à moins que a ne soit égal à 1 ou à $p-1$. Si, en effet, on a $\alpha = a$, $a^2-1=(a-1)(a+1)$ est divisible par p; or p est premier, il divise donc $a-1$ ou $a+1$, et, comme a est $<p$, on a nécessairement $a=1$ ou $a=p-1$.

Il résulte de là que les nombres

$$2,\ 3,\ 4,\ \ldots,\ (p-2)$$

peuvent être associés deux à deux, de manière que le produit des deux *associés* soit congru à l'unité, et, en multipliant entre elles les congruences ainsi obtenues, on aura

$$2.3.4\ldots(p-2) \equiv 1 \pmod{p};$$

multipliant enfin par $p-1$, on a

$$1.2.3.4\ldots(p-1) \equiv p-1 \pmod{p},$$

ou

$$1.2.3.4\ldots(p-1)+1 \equiv 0 \pmod{p},$$

ce qu'il fallait démontrer.

Ce théorème est surtout remarquable en ce qu'il exprime une propriété qui appartient exclusivement aux nombres premiers; car, si p est un nombre composé, et que θ soit un de ses diviseurs, θ divisera le produit $1.2.3\ldots(p-1)$, et, par conséquent, il ne pourra diviser ce même produit augmenté de l'unité. Il en sera donc de même du nombre p.

Corollaire. — *Tout nombre premier p de la forme $4n+1$ est la somme de deux carrés.*

En effet, par le théorème précédent, p divise la somme

$$1.2.3\ldots 2n(2n+1)\ldots(4n)+1;$$

mais les nombres

$$2n+1,\ 2n+2,\ \ldots,\ 4n$$

sont respectivement congrus à

$$-2n,\ -(2n-1),\ \ldots,\ -1$$

suivant le module p; donc le produit des uns est congru au produit des autres. D'ailleurs le nombre des facteurs étant pair, on peut changer leurs signes, et l'on a

$$(1.2.3\ldots 2n)^2+1\equiv 0 \pmod{p};$$

p divise ainsi la somme de deux carrés, et, par conséquent, il est lui-même la somme de deux carrés (n° 15).

Remarque. — Un nombre de la forme $4n+3$ ne peut être la somme de deux carrés. En effet, tout carré pair a la forme $4n$, et tout carré impair est de la forme $4n+1$; par conséquent, la somme de deux carrés premiers entre eux a toujours l'une des deux formes $4n+1$ et $4n+2$.

Deuxième démonstration. — On peut encore démontrer le théorème de Wilson au moyen de la formule

$$\Delta^n u_0 = u_n - \frac{n}{1}u_{n-1} + \frac{n(n-1)}{1.2}u_{n-2} - \ldots + (-1)^n u_0$$

que nous avons établie au n° 152, et qui exprime la différence $n^{\text{ième}}$ du terme u_0 de la suite

$$u_0,\ u_1,\ u_2,\ u_3,\ \ldots.$$

Si l'on suppose généralement

$$u_\mu = (x+\mu)^n,$$

on aura

$$\Delta^n u_\mu = 1.2.3\ldots n,$$

et notre formule générale deviendra

$$1.2\ldots n = (x+n)^n - \frac{n}{1}(x+n-1)^n + \frac{n(n-1)}{1.2}(x+n-2)^n - \ldots + (-1)^n x^n.$$

Soit maintenant $x = 1$, $n = p-1$, p étant un nombre premier, il viendra

$$1.2.3\ldots(p-1) = p^{p-1} - \frac{p-1}{1}(p-1)^{p-1} + \frac{(p-1)(p-2)}{1.2}(p-2)^{p-1} - \ldots - \frac{p-1}{1}2^{p-1} + 1^{p-1};$$

on a d'ailleurs

$$0 = (1-1)^{p-1} = 1 - \frac{p-1}{1} + \frac{(p-1)(p-2)}{1.2} - \ldots + 1,$$

d'où

$$1.2.3\ldots(p-1)+1 = p^{p-1} - \frac{p-1}{1}[(p-1)^{p-1}-1] + \frac{(p-1)(p-2)}{1.2}[(p-2)^{p-1}-1] + \ldots - \frac{p-1}{1}(2^{p-1}-1).$$

Dans le second membre de cette formule, le premier terme est une puissance de p et tous les termes qui suivent sont divisibles par p, d'après le théorème de Fermat; on a donc

$$1.2.3\ldots(p-1)+1 \equiv 0 \pmod{p}.$$

Théorème de Fermat généralisé.

295. Le théorème de Fermat est susceptible d'être étendu aux modules composés : il n'est effectivement qu'un cas particulier de la proposition suivante :

THÉORÈME. — *Si a et M sont des nombres premiers entre eux, et que $\varphi(M)$ exprime combien il y a de nombres premiers à M et non supérieurs à ce nombre, la différence*

$$a^{\varphi(M)} - 1$$

sera divisible par M; en d'autres termes, on aura

$$a^{\varphi(M)} - 1 \equiv 0 \pmod{M}.$$

La première des démonstrations dont nous avons fait usage au n° 293 s'applique au cas actuel, avec de légères modifications. Soient

$$(1) \qquad \alpha, \beta, \gamma, \delta, \ldots, \omega$$

les $\varphi(M)$ nombres premiers à M et non supérieurs à M. Si on les multiplie par le nombre a qui est également premier à M, on obtiendra la nouvelle suite

$$(2) \qquad a\alpha, a\beta, a\gamma, a\delta, \ldots, a\omega;$$

aucun terme de la suite (2), $a\alpha$ par exemple, ne peut être divisible par M; car M est premier à a et il est supérieur à α; pour la même raison, la différence $a(\beta - \alpha)$ de deux termes de la suite (2) ne peut être divisible par M, d'où il résulte que, si l'on prend les résidus minima, relativement à M, des termes de la suite (2), on obtiendra $\varphi(M)$ résultats différents. En outre, les nombres (2) sont premiers à M, et en conséquence leurs résidus le sont aussi ; ces résidus sont donc précisément les

nombres (1). Les nombres (2) étant respectivement congrus aux nombres (1), le produit des uns est congru au produit des autres, et l'on a

$$\alpha\beta\gamma\ldots\omega\,[a^{\varphi(M)}-1]\equiv 0 \pmod{M};$$

en divisant par le produit $\alpha\beta\gamma\ldots\omega$ qui est premier avec le module, il vient enfin

$$a^{\varphi(M)}-1\equiv 0 \pmod{M}.$$

Théorème de Wilson généralisé.

296. Le théorème de Wilson est lui-même susceptible d'être généralisé; on peut effectivement l'énoncer comme il suit :

Théorème. — *Si* P *désigne le produit des* $\varphi(M)$ *nombres premiers à* M *et non supérieurs à* M, *on a*

$$P\equiv\mp 1 \pmod{M},$$

savoir

$$P\equiv -1 \pmod{M},$$

si M *est égal à une puissance d'un nombre premier impair, ou égal au double d'une telle puissance ou égal à* 4; *et*

$$P\equiv +1 \pmod{M},$$

dans tous les autres cas.

En effet, soient, comme précédemment,

(1) $\alpha,\ \beta,\ \gamma,\ \ldots,\ \omega$

les nombres premiers à M et non supérieurs à M. Si a désigne l'un de ces nombres, les produits

(2) $a\alpha,\ a\beta,\ a\gamma,\ \ldots,\ a\omega$

donneront, comme on l'a vu, des résidus minima diffé-

rents, relativement au module M. Parmi ces résidus, il y en aura donc un égal à 1, et un autre égal à $M-1$. Supposons que $a\alpha$ donne le résidu 1; si a et α sont inégaux, je dirai que ces nombres sont *associés du premier genre*. Si $\alpha=a$, le produit $a\times a$ donnant le résidu 1, le produit $a(M-a)$ donnera le résidu -1 ou $M-1$; je dirai alors que a et $M-a$ sont *associés du second genre*. Il résulte de cette définition que deux associés du second genre constituent un couple de racines conjuguées de la congruence

$$(3) \qquad x^2-1\equiv 0 \pmod{M}.$$

Il est évident que le produit de tous ceux des nombres (1) qui composent les couples d'associés du premier genre est congru à 1, suivant le module M, tandis que le produit de tous ceux qui forment les couples du deuxième genre est congru à $(-1)^\mu$, μ désignant le nombre des couples de racines conjuguées de la congruence (3). Il résulte de là que l'on a

$$P\equiv(-1)^\mu \pmod{M}.$$

Or, si l'on a $M=p^\nu$, ou $M=2p^\nu$, ou $M=4$, p étant un nombre premier impair, le nombre μ est égal à 1, tandis que le même nombre est pair dans tous les autres cas (nº 292); donc on a

$$P\equiv-1 \pmod{M},$$

dans les trois cas de $M=p^\nu$, $=2p^\nu$, $=4$, et

$$P\equiv+1 \pmod{M},$$

quand le module M n'est pas de l'une de ces trois formes.

REMARQUE. — Si l'on veut avoir l'associé d'un nombre a,

il suffira de déterminer la racine de la congruence

$$ax - 1 \equiv 0 \pmod{M},$$

ou, si l'on veut, de résoudre en nombres entiers l'équation indéterminée

$$ax - My = 1.$$

Au surplus, comme le théorème de Fermat généralisé donne

$$a^{\varphi(M)} \equiv 1 \pmod{M},$$

l'associé demandé est évidemment le résidu de la puissance

$$a^{\varphi(M)-1}.$$

Des congruences dont le module est un nombre premier.

297. Étant donnée la congruence

$$A_0 x^m + A_1 x^{m-1} + \ldots + A_{m-1} x + A_m \equiv 0 \pmod{p},$$

dont le module p est supposé premier, et dans laquelle les coefficients $A_0, A_1, \ldots$ sont des entiers compris entre zéro et p ou entre $-\frac{p}{2}$ et $+\frac{p}{2}$, on peut toujours la remplacer par une autre dont le premier terme ait pour coefficient l'unité. Car soit A' le nombre associé de A_0, c'est-à-dire le nombre tel que l'on ait

$$A_0 A' \equiv 1 \pmod{p},$$

et désignons par

$$P_1, P_2, \ldots, P_m$$

les résidus des produits

$$A' A_1, A' A_2, \ldots, A' A_m;$$

si l'on multiplie par $A_0 A'$ les termes de la congruence proposée, à partir du deuxième, cette congruence pren-

dra la forme

$$A_0(x^m+P_1x^{m-1}+P_2x^{m-2}+\ldots+P_{m-1}x+P_m)\equiv 0 \pmod{p},$$

et, en divisant par A_0 qui est premier avec le module, il viendra

$$x^m+P_1x^{m-1}+P_2x^{m-2}+\ldots+P_{m-1}x+P_m\equiv 0 \pmod{p}.$$

298. Les congruences dont le module est premier jouissent d'une propriété très-importante et qui est exprimée par la proposition suivante :

Théorème. — *Une congruence non identique suivant un module premier ne peut avoir plus de racines qu'il n'y a d'unités dans son degré.*

Soit

$$(1)\qquad f(x)\equiv 0 \pmod{p}$$

une congruence de degré m suivant le module premier p, $f(x)$ désignant, pour abréger, le polynôme

$$f(x)=A_0x^m+A_1x^{m-1}+\ldots+A_{m-1}x+A_m,$$

dans lequel les coefficients sont des nombres entiers compris entre zéro et p ou entre $-\frac{p}{2}$ et $+\frac{p}{2}$.

Si l'on désigne par $a_1, a_2, \ldots, a_m$ des nombres entiers quelconques et que l'on pose, comme au n° 45,

$$(2)\qquad \begin{cases} f(x)=(x-a_1)f_1(x)+R_1,\\ f_1(x)=(x-a_2)f_2(x)+R_2,\\ f_2(x)=(x-a_3)f_3(x)+R_3,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ f_{m-1}(x)=(x-a_m)f_m(x)+R_m, \end{cases}$$

$R_1, R_2, \ldots, R_m$ étant indépendants de x, puis que l'on ajoute toutes ces égalités, après les avoir multipliées respectivement par les m facteurs

$$1,\ x-a_1,\ (x-a_1)(x-a_2),\ \ldots,\ (x-a_1)\ldots(x-a_{m-1}),$$

il viendra, en remplaçant $f^m(x)$ par sa valeur A_0,

$$(3)\quad \begin{cases} f(x) = A_0(x-a_1)(x-a_2)\ldots(x-a_m) \\ \qquad + R_m(x-a_1)(x-a_2)\ldots(x-a_{m-1}) + \ldots \\ \qquad + R_3(x-a_1)(x-a_2) + R_2(x-a_1) + R_1. \end{cases}$$

Supposons maintenant que la congruence proposée ait une racine, et prenons a_1 égal à cette racine; on aura alors

$$R_1 \equiv 0 \pmod{p},$$

et, d'après les égalités (2), la congruence (1) pourra se mettre sous la forme

$$(x-a_1)f_1(x) \equiv 0 \pmod{p}.$$

Le module p étant premier, le produit $(x-a_1)f_1(x)$ ne peut être congru à zéro suivant ce module, à moins que l'un des facteurs ne soit divisible par p; donc, si la précédente congruence admet des racines distinctes de a_1, ces racines appartiendront à la congruence

$$(4)\qquad f_1(x) \equiv 0 \pmod{p}.$$

Si la congruence (4) n'a point de racines, la proposée n'aura que la seule racine a_1. Si, au contraire, cette congruence a des racines, et que l'on prenne pour a_2 l'une de ces racines, on aura

$$R_2 \equiv 0 \pmod{p},$$

et, d'après les égalités (2), la congruence (4) prendra la forme

$$(x-a_2)f_2(x) \equiv 0 \pmod{p}.$$

Le même raisonnement montre que, si cette congruence a des racines distinctes de a_2, ces racines appartiennent à la congruence

$$f_2(x) \equiv 0 \pmod{p}.$$

On voit que, généralement, si chacune des congruences

$$f(x) \equiv 0,\quad f_1(x) \equiv 0,\quad \ldots,\quad f_{m-\mu-1}(x) \equiv 0 \pmod{p}$$

a une racine, et que la congruence

$$f_{m-\mu}(x) \equiv 0 \pmod{p}$$

n'en ait aucune, la proposée aura $m-\mu$ racines. Si l'on suppose que $a_1, a_2, \ldots, a_{m-\mu}$ soient ces racines, on aura

$$R_1 \equiv 0,\ R_2 \equiv 0,\ \ldots,\ R_{m-\mu} \equiv 0 \pmod{p},$$

et la formule (3) donnera

$$(5)\quad f(x) \equiv (x-a_1)(x-a_2)\ldots(x-a_{m-\mu})\,F(x) \pmod{p},$$

$F(x)$ désignant une fonction entière du degré μ, telle que la congruence

$$F(x) \equiv 0 \pmod{p}$$

n'ait aucune racine.

Si le nombre μ est égal à zéro, la fonction $F(x)$ se réduit à la constante A_0, et la formule (3) donne

$$(6)\quad f(x) \equiv A_0(x-a_1)(x-a_2)\ldots(x-a_m) \pmod{p},$$

d'où il suit que la congruence proposée ne peut avoir pour racines que les m nombres $a_1, a_2, \ldots, a_m$.

Corollaire. — *Si la congruence $f(x) \equiv 0 \pmod{p}$ du degré m est satisfaite par plus de m valeurs de x, elle est nécessairement identique.*

299. Nous présenterons ici une conséquence fort importante du théorème que nous venons d'établir.

Théorème. — *Si $f(x)$ et $F(x)$ sont des fonctions entières à coefficients entiers, dont les degrés soient inférieurs à p, et que $f(x)$ soit un diviseur de la fonction*

$x^{p-1} - 1 + p\,F(x)$, *p étant un nombre premier, la congruence*

$$f(x) \equiv 0 \pmod{p}$$

aura précisément autant de racines qu'il y a d'unités dans le nombre qui exprime son degré.

En effet, d'après le théorème de Fermat, la congruence

$$(1) \qquad x^{p-1} - 1 \equiv 0 \pmod{p}$$

a les $p - 1$ racines

$$1,\ 2,\ 3,\ \ldots,\ (p-1).$$

D'ailleurs, si l'on a

$$(2) \qquad x^{p-1} - 1 + pF(x) = f(x) f_1(x),$$

$f(x)$ et $f_1(x)$ étant des polynômes à coefficients entiers, la congruence (1) peut se mettre sous la forme

$$f(x) f_1(x) \equiv 0 \pmod{p},$$

et chacune de ses racines appartient à l'une ou à l'autre des deux

$$(3) \qquad f(x) \equiv 0, \quad f_1(x) \equiv 0 \pmod{p}.$$

Or, si l'une des congruences (3) avait moins de racines qu'il n'y a d'unités dans son degré, il faudrait que l'autre en eût plus qu'il n'y a d'unités dans le sien, ce qui est impossible ; le théorème énoncé est donc établi.

300. On peut déduire du théorème précédent un procédé très-simple pour déterminer le nombre des racines d'une congruence de module premier. Démontrons d'abord le lemme suivant :

Lemme. — *Si $f_2(x)$ désigne le reste de la division des deux polynômes $f(x)$ et $f_1(x)$, dont les premiers termes*

ont pour coefficient l'unité, les racines communes aux deux congruences

$$f(x) \equiv 0 \pmod{p}, \quad f_1(x) \equiv 0 \pmod{p}$$

sont les mêmes que les racines communes à

$$f_1(x) \equiv 0 \pmod{p}, \quad f_2(x) \equiv 0 \pmod{p}.$$

Soit Q le quotient de la division de $f(x)$ par $f_1(x)$, on aura

$$f(x) = f_1(x).Q + f_2(x),$$

et cette égalité fait voir que, si $f_1(x)$ est divisible par p en même temps que l'un des deux polynômes $f(x)$ et $f_2(x)$, l'autre le sera nécessairement aussi; d'où résulte la proposition énoncée.

Corollaire. — *Les racines communes à deux congruences*

$$f(x) \equiv 0, \quad f_1(x) \equiv 0 \pmod{p}$$

appartiennent à la congruence

$$\varphi(x) \equiv 0 \pmod{p},$$

$\varphi(x)$ *désignant le plus grand commun diviseur aux deux polynômes* $f(x)$ *et* $f_1(x)$.

Remarque. — Pour trouver ce plus grand commun diviseur $\varphi(x)$, on suivra la marche ordinaire; seulement on négligera tous les termes qui sont multipliés par p. Il faut, en outre, que toutes les divisions puissent se faire sans écrire de coefficients fractionnaires. Pour cela, on peut faire en sorte, comme il a été indiqué plus haut, que chaque reste soit divisible par le coefficient de son premier terme, et alors on fera abstraction de ce diviseur commun. On arrive aussi au même but en multipliant chaque dividende par un facteur convenable, ou même simplement en ajoutant au coefficient du premier terme de chaque dividende un multiple de p tel, qu'après cette

addition le premier terme du dividende en question soit divisible par le premier terme du diviseur correspondant.

301. Supposons maintenant qu'on veuille connaître le nombre des racines de la congruence

$$(1) \qquad f(x) \equiv 0 \pmod{p}.$$

Ces racines appartiennent toutes à la congruence

$$(2) \qquad x^{p-1} - 1 \equiv 1 \pmod{p};$$

il suffit donc de chercher les racines communes aux congruences (1) et (2). Pour cela, on déterminera, comme il vient d'être dit, le plus grand commun diviseur à $f(x)$ et à $x^{p-1}-1$. S'il n'existe pas de diviseur commun, la proposée n'aura aucune racine; si, au contraire, on trouve un plus grand commun diviseur $\varphi(x)$ de degré μ, la congruence proposée aura μ racines, qui seront celles de la congruence

$$\varphi(x) \equiv 0 \pmod{p},$$

laquelle a effectivement μ racines, puisque $\varphi(x)$ est un diviseur de degré μ du binôme $x^{p-1}-1$.

Exemple. — On demande le nombre des racines de la congruence

$$f(x) = x^5 - 3x^4 - 2x^3 - 2x^2 + x - 2 \equiv 0 \pmod{7}.$$

En cherchant le plus grand commun diviseur des polynômes x^6-1 et $f(x)$, comme on l'a indiqué au nº 300, on trouve les deux restes

$$-3(x^4+2x^3+3x^2-2x+3),$$
$$2(x^3+3x^2-x-3);$$

le second reste étant diviseur du premier, la congruence proposée a trois racines qui appartiennent aussi à la congruence du troisième degré

$$x^3+3x^2-x-3 \equiv 0 \pmod{7}.$$

Nouvelle démonstration du théorème de Wilson.

302. Si p est un nombre premier, la congruence

$$(x-1)(x-2)(x-3)\ldots(x-p+1)-(x^{p-1}-1)\equiv 0 \pmod{p}$$

admet les $p-1$ racines

$$1,\ 2,\ 3,\ \ldots,\ (p-1);$$

et, comme elle n'est que du degré $p-2$, elle doit être identique. Si donc on désigne par S_1 la somme des nombres $1, 2, \ldots, (p-1)$, par S_2 la somme de leurs produits deux à deux, etc., par S_{p-1} le produit de tous ces nombres, on aura

$$S_1\equiv 0,\ S_2\equiv 0,\ S_3\equiv 0,\ \ldots,\ S_{p-1}\equiv -1,$$

suivant le module p. La dernière de ces congruences constitue le théorème de Wilson.

Remarque. — Les coefficients de l'équation

$$(x-1)(x-2)(x-3)\ldots(x-p+1)=0,$$

ordonnée par rapport à x, étant des multiples de p, à l'exception du dernier terme, si p est premier, la somme des puissances $m^{\text{ièmes}}$ des $p-1$ racines

$$1,\ 2,\ 3,\ 4,\ \ldots,\ (p-1)$$

sera divisible par p, à moins que m ne soit un multiple de $p-1$. Cela résulte immédiatement des formules de Newton.

CHAPITRE II.

DES RÉSIDUS DES PUISSANCES ET DES CONGRUENCES BINOMES.

Des nombres qui appartiennent à un exposant donné relativement à un module donné.

303. Le nombre a étant premier avec le module M, considérons la suite indéfinie des puissances de a, savoir

(1) $$1,\ a,\ a^2,\ a^3,\ \ldots,\ a^n,\ \ldots.$$

Comme cette suite renferme un nombre illimité de termes, et qu'on ne peut trouver qu'un nombre limité $\varphi(M)$ de résidus distincts, il y aura nécessairement deux puissances, telles que a^ν et $a^{n+\nu}$, qui seront congrues suivant le module M. On peut diviser la congruence

(2) $$a^{n+\nu} \equiv a^\nu \pmod{M}$$

par a^ν, qui est un nombre premier au module, et il vient alors

(3) $$a^n \equiv 1 \pmod{M}.$$

Réciproquement, si la congruence (3) a lieu, la congruence (2) aura lieu aussi, quel que soit l'exposant ν.

Il résulte de là que, si n est le plus petit nombre tel que la congruence (3) ait lieu, les résidus de la série (1) formeront une suite périodique dont la période comprendra n termes incongrus suivant le module M, et qui seront les résidus des puissances

$$1,\ a,\ a^2,\ \ldots,\ a^{n-1}.$$

Ceux des termes de la série (1), autres que l'unité, qui donnent le résidu (1), sont, d'après cela,

$$a^n,\quad a^{2n},\quad a^{3n},\quad \ldots;$$

or, d'après le théorème de Fermat généralisé, on a

$$a^{\varphi(\mathrm{M})} \equiv 1 \pmod{\mathrm{M}}:$$

donc $\varphi(\mathrm{M})$ est un multiple de n.

Lorsque n désigne le plus petit nombre positif, tel que $a^n \equiv 1 \pmod{\mathrm{M}}$, on dit que le nombre a *appartient à l'exposant n, relativement au module* M. On peut alors énoncer cette proposition :

Théorème. — *L'exposant auquel appartient, relativement au module* M, *un nombre quelconque premier avec ce module, est un diviseur de* $\varphi(\mathrm{M})$.

304. On peut encore arriver à ce résultat par une autre méthode qui ne suppose pas le théorème de Fermat et qui conduit même à une démonstration nouvelle de ce théorème.

Quel que soit l'entier a premier avec le module M, la suite des puissances

$$(1)\qquad 1,\ a,\ a^2,\ a^3,\ \ldots,\ a^n,\ \ldots$$

donne, comme nous venons de le dire, un certain nombre n de résidus distincts qui sont ceux des puissances

$$(2)\qquad 1,\ a,\ a^2,\ a^3,\ \ldots,\ a^{n-1},$$

et n est le plus petit nombre tel que l'on ait

$$(3)\qquad a^n \equiv 1 \pmod{\mathrm{M}}.$$

Si la suite des résidus des nombres (2) embrasse tous les nombres premiers et non supérieurs à M, on aura

$$\varphi(\mathrm{M}) = n;$$

dans le cas contraire, soit b l'un des nombres premiers à M, qui ne sont congrus, suivant ce module, à aucun des termes de la suite (2). En multipliant par b les termes de cette suite, on en obtient une deuxième

(4) $$b,\ ba,\ ba^2,\ \ldots,\ ba^{n-1}$$

dont tous les termes sont distincts; car, si l'on avait

$$ba^\mu \equiv ba^\nu \pmod{M},$$

il en résulterait

$$a^\mu \equiv a^\nu \pmod{M},$$

ce qui est contre l'hypothèse. On voit aussi que les termes de la suite (4) sont incongrus, suivant le module M, aux termes de la suite (2); car, si l'on avait

$$ba^\mu \equiv a^\nu \pmod{M},$$

il en résulterait

$$b \equiv a^{\nu-\mu} \quad \text{ou} \quad \equiv a^{n+\nu-\mu} \pmod{M},$$

ce qui est encore contre l'hypothèse. Ainsi l'on a

$$\varphi(M) = 2n \quad \text{ou} \quad \varphi(M) > 2n.$$

Si $\varphi(M)$ est $> 2n$, soit c l'un des nombres premiers et non supérieurs à M, qui ne sont pas compris parmi les résidus des suites (2) et (4). En multipliant la suite (2) par c, on obtient une nouvelle suite

(5) $$ca,\ ca^2,\ ca^3,\ \ldots,\ ca^{n-1},$$

dont les termes sont incongrus à ceux de la suite (2), d'après ce qui précède, et j'ajoute qu'ils le sont aussi aux termes de la suite (4); car, si l'on avait

$$ca^\mu \equiv ba^\nu \pmod{M},$$

on en conclurait

$$c \equiv ba^{\nu-\mu} \quad \text{ou} \quad \equiv ba^{n+\nu-\mu} \pmod{M},$$

et le nombre c serait compris parmi les résidus de la suite (4), ce qui est contre l'hypothèse. D'après cela, on a

$$\varphi(M) = 3n \quad \text{ou} \quad \varphi(M) > 3n.$$

On peut continuer ainsi jusqu'à l'épuisement complet des $\varphi(M)$ nombres premiers et non supérieurs à M, et l'on voit que l'on a nécessairement

$$\varphi(M) = mn,$$

m étant un nombre entier; ce qui est le théorème démontré au numéro précédent.

Mais la congruence (3) entraîne nécessairement

$$a^{mn} \equiv 1 \pmod{M},$$

ou

$$a^{\varphi(M)} \equiv 1 \pmod{M},$$

ce qui est précisément le théorème de Fermat généralisé.

Des racines primitives.

305. D'après le théorème de Fermat généralisé, la congruence

$$x^{\varphi(M)} \equiv 1 \pmod{M}$$

admet pour racines les $\varphi(M)$ nombres premiers et non supérieurs à M. Ceux de ces nombres qui appartiennent, suivant le module M, à l'exposant $\varphi(M)$ sont dits *racines primitives* de la précédente congruence, ou simplement *racines primitives, relativement au module* M.

Ainsi le nombre a, premier à M, sera racine primitive si, pour toutes les valeurs de n inférieures à $\varphi(M)$, a^n est incongrue à l'unité, suivant le module M. Dans ce cas, la série des résidus des puissances

$$1,\ a,\ a^2,\ \ldots,\ a^{\varphi(M)-1}$$

embrasse les $\varphi(M)$ nombres premiers à M et non supérieurs à M.

On peut établir de suite qu'il n'existe de racines primitives que dans des cas peu étendus.

Le module M étant décomposé en facteurs premiers, soit

$$M = p^{\nu} q^{\mu} r^{\lambda}, \ldots,$$

$p, q, r, \ldots$ étant des nombres premiers inégaux. Tout nombre a, premier à M, sera premier avec chacun des facteurs $p^{\nu}, q^{\mu}, r^{\lambda}, \ldots$ et l'on aura, par le théorème de Fermat généralisé,

$$a^{\varphi(p^{\nu})} \equiv 1 \pmod{p^{\nu}},$$
$$a^{\varphi(q^{\mu})} \equiv 1 \pmod{q^{\mu}},$$
$$a^{\varphi(r^{\lambda})} \equiv 1 \pmod{r^{\lambda}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots;$$

Si S désigne le plus petit des nombres divisibles par chacun des suivants :

$$\varphi(p^{\nu}) = p^{\nu-1}(p-1),$$
$$\varphi(q^{\mu}) = q^{\mu-1}(q-1),$$
$$\varphi(r^{\lambda}) = r^{\lambda-1}(r-1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$

on aura aussi

$$a^{S} \equiv 1 \pmod{p^{\nu}}, \quad a^{S} \equiv 1 \pmod{q^{\mu}}, \quad a^{S} \equiv 1 \pmod{r^{\lambda}}, \ldots.$$

La différence $a^{S} - 1$ étant ainsi divisible par chacun des nombres $p^{\nu}, q^{\mu}, r^{\lambda}, \ldots$, elle le sera par le produit M des mêmes nombres, et l'on aura

$$a^{S} \equiv 1 \pmod{M}.$$

Or, $\varphi(p^{\nu})$ est un nombre pair, sauf le seul cas où l'on

a $p = 2$, $\nu = 1$; de même $\varphi(q^\mu)$ est pair, à moins que $q = 2$, $\mu = 1$, et ainsi de suite. Donc, si M renferme plus d'un facteur premier impair, ou si, ne contenant qu'un seul facteur premier impair, il renferme le facteur 2 à une puissance supérieure à la première, deux au moins des nombres

$$\varphi(p^\nu), \quad \varphi(q^\mu), \quad \varphi(r^\lambda), \ldots$$

auront un diviseur commun, et, par conséquent, le plus petit commun multiple de ces nombres sera inférieur à leur produit. Ainsi l'on aura

$$S < \varphi(M),$$

et le nombre a, pour lequel on a $a^S \equiv 1 \pmod{M}$, ne sera pas racine primitive relativement au module M.

Il reste à examiner le cas où M ne renferme aucun facteur premier impair; on a alors

$$M = 2^\nu, \quad \varphi(M) = 2^{\nu-1},$$

et je dis qu'il n'y a point de racines primitives, si ν est supérieur à 2.

En effet, tout nombre impair a peut être représenté par la formule

$$a = \pm 1 + 2^2 k,$$

et, par des élévations au carré successives, on en déduit

$$a^2 = 1 + 2^3 k_1,$$
$$a^{2^2} = 1 + 2^4 k_2,$$
$$a^{2^3} = 1 + 2^5 k_3, \ldots,$$
$$a^{2^{\nu-2}} = 1 + 2^\nu k_{\nu-2},$$

$k_1, k_2, \ldots, k_{\nu-2}$ étant des nombres entiers. La dernière de ces égalités peut s'écrire

$$a^{\frac{1}{2}\varphi(M)} \equiv 1 \quad (\text{mod. } M),$$

si ν est > 2, et en conséquence a n'est pas racine primitive.

Il résulte de là qu'il ne peut exister de racines primitives que dans les trois cas suivants :

1° *Si le module* M *est un nombre premier impair ou une puissance d'un nombre premier impair ;*

2° *Si le module* M *est égal au double d'une puissance d'un nombre premier impair ;*

3° *Si le module* M *est égal à* 4.

Dans le cas de $M = 4$, on a $\varphi(M) = 2$, et le nombre -1 ou 3 satisfait évidemment à la définition des racines primitives. Le cas où M est une puissance de 2 supérieure à 4 mérite une attention particulière, bien qu'il n'y ait point de racines primitives, dans le sens que nous attachons à ce terme.

Des racines primitives, dans le cas où le module est un nombre premier impair.

306. Lorsque le module M se réduit à un nombre premier impair p, on a $\varphi(M) = p - 1$. Dans ce cas, il existe toujours des racines primitives et il est facile d'en déterminer le nombre par le théorème suivant, dont nous empruntons la démonstration à Gauss :

Théorème. — *Si le nombre p est premier, et que n désigne un diviseur quelconque de $p-1$, il y a précisément $\varphi(n)$ nombres qui appartiennent à l'exposant n; le symbole $\varphi(n)$ exprimant combien il y a de nombres premiers et non supérieurs à n.*

Supposons qu'il existe un nombre a appartenant à l'exposant n, suivant le module p; les résidus des puissances

$$(1) \qquad 1, a, a^2, \ldots, a^{n-1}$$

seront distincts et chacun d'eux sera la racine de la congruence

$$(2)\qquad x^n - 1 \equiv 0 \pmod{p};$$

car l'hypothèse

$$a^n \equiv 1 \pmod{p}$$

entraîne

$$(3)\qquad a^{ne} \equiv 1 \pmod{p},\quad \text{ou}\quad (a^e)^n - 1 \equiv 0 \pmod{p},$$

e étant l'un quelconque des nombres

$$0,\ 1,\ 2,\ \ldots,\ n-1;$$

donc, d'après le théorème du nº 298, la congruence (2) n'a pas d'autres racines que les résidus des puissances contenues dans la suite (1). Par conséquent, s'il existe des nombres, autres que a, qui appartiennent à l'exposant n, chacun d'eux doit être congru, suivant le module p, à une puissance telle que a^e.

Désignons par m l'exposant auquel appartient a^e; d'après la congruence (3), n sera un multiple de m; on a d'ailleurs

$$(4)\qquad (a^e)^m \equiv 1 \pmod{p}\quad \text{ou}\quad a^{me} \equiv 1 \pmod{p},$$

et comme a appartient à l'exposant n, il en résulte que me est un multiple de n. Cela exige que m soit un multiple de n, quand e est premier à n; les nombres m et n étant alors divisibles l'un par l'autre, ils sont égaux entre eux. Donc a^e appartient à l'exposant n, si e est premier avec n; mais, si les nombres e et n ont un diviseur commun θ supérieur à 1, la congruence

$$\left(a^{\frac{e}{\theta}}\right)^n \equiv 1 \pmod{p}$$

peut s'écrire

$$(a^e)^{\frac{n}{\theta}} \equiv 1 \pmod{p},$$

ce qui montre que a^e appartient à un exposant moindre que n.

On peut conclure de là que, s'il existe un nombre appartenant à l'exposant n, suivant le module p, il y a précisément $\varphi(n)$ nombres qui appartiennent à cet exposant.

Cela posé, l'exposant auquel appartient l'un quelconque des nombres

$$(5) \qquad 1,\ 2,\ 3,\ \ldots,\ (p-1),$$

relativement au module p, est, comme on sait, égal à l'un des diviseurs

$$(6) \qquad d,\ d',\ d'',\ d''',\ \ldots$$

du nombre $p-1$. Si l'on emploie le symbole $\psi(d)$ pour exprimer combien il y a, dans la suite (5), de nombres qui appartiennent à l'exposant d, on aura, d'après ce qui précède,

$$\psi(d) = \varphi(d) \quad \text{ou} \quad \psi(d) = 0.$$

Pareillement, $\psi(d')$, $\psi(d'')$, ... exprimeront combien il y a, dans la suite (5), de nombres qui appartiennent aux exposants d', d'', ... respectivement. L'unité fait partie de la suite des diviseurs (6), et comme 1 est évidemment le seul nombre qui appartient à l'exposant 1, on a

$$\psi(1) = 1.$$

Enfin le nombre des termes de la suite (5) étant $p-1$, et chacun d'eux appartenant à l'un des exposants contenus dans la suite (6), on a l'identité

$$\psi(d) + \psi(d') + \psi(d'') + \ldots = p - 1.$$

Mais on a aussi (n° 286)

$$\varphi(d) + \varphi(d') + \varphi(d'') + \ldots = p - 1:$$

donc

$$(7) \quad \psi(d) + \psi(d') + \psi(d'') + \ldots = \varphi(d) + \varphi(d') + \varphi(d'') + \ldots.$$

Dans le premier membre de cette égalité, ceux des termes qui ne sont pas nuls sont respectivement égaux, d'après ce qui précède, aux termes qui occupent les mêmes rangs, dans le second membre; on peut donc supprimer de part et d'autre ces termes égaux. Mais, après cette suppression, il reste zéro dans le premier membre de l'égalité (7); donc il ne doit rien rester dans le second membre. D'où il suit que la suppression a porté sur tous les termes, et que l'on a

$$\psi(d) = \varphi(d),$$

quel que soit le diviseur d.

Corollaire. — *Il y a $\varphi(p-1)$ nombres qui appartiennent à l'exposant $p-1$, relativement au module premier p; en d'autres termes, il y a, relativement à ce module, $\varphi(p-1)$ racines primitives.*

Remarque. — Les nombres qui appartiennent, suivant le module premier p, à un exposant n égal à un diviseur quelconque de $p-1$, sont dits quelquefois *racines primitives pour la congruence* $x^n \equiv 1 \pmod{p}$. Alors, d'après ce qui précède, cette congruence a n racines, parmi lesquelles il y en a $\varphi(n)$ qui sont primitives.

307. Nous établirons encore ici une proposition fort importante qui trouvera plus loin son application.

Théorème. — *Si deux nombres a et b appartiennent, relativement au module premier p, à deux exposants m et n premiers entre eux, le produit ab appartient à l'exposant mn.*

En effet, soit s un exposant tel que

$$(ab)^s = a^s b^s \equiv 1 \pmod{p},$$

on aura, par l'élévation à la puissance m,

$$a^{ms} b^{ms} \equiv 1 \pmod{p};$$

mais, a appartenant à l'exposant m, on a

$$a^{ms} \equiv 1 \quad (\text{mod.}\, p):$$

donc

$$b^{ms} \equiv 1 \quad (\text{mod.}\, p),$$

et, par conséquent, ms est un multiple de l'exposant n auquel b appartient. D'ailleurs m et n sont premiers entre eux; donc s est un multiple de n. On ferait voir de même que s est un multiple de m, et il en résulte que s est divisible par le produit mn. Or on a, par hypothèse,

$$a^m \equiv 1, \quad b^n \equiv 1 \quad (\text{mod.}\, p),$$

d'où

$$a^{mn} b^{mn} = (ab)^{mn} \equiv 1 \quad (\text{mod.}\, p):$$

donc le produit mn est bien l'exposant auquel ab appartient.

Corollaire I. — *Si les nombres a, b, c, ... appartiennent respectivement, par rapport au module p, aux exposants m, n, r, ..., premiers entre eux deux à deux, le produit abc... appartient à l'exposant mnr....*

Corollaire II. — *Si le nombre $p-1$ est égal au produit $2^\varrho q^\lambda r^\mu$, ..., q, r, ... étant des nombres premiers impairs inégaux, et si a, b, c, ... désignent des nombres qui appartiennent respectivement aux exposants 2^ϱ, q^λ, r^μ, ..., le produit abc... ou son résidu appartient à l'exposant $p-1$, et il est en conséquence racine primitive, relativement au module p.*

Autre manière de présenter les résultats qui précèdent.

308. Les propriétés que nous venons d'établir, à l'égard des modules premiers, peuvent encore être démontrées, comme nous allons le faire voir, par une méthode identique à celle dont nous avons fait usage dans le Cha-

pitre V de la Section I, en nous occupant des racines des équations binômes; il y a quelque avantage à faire ressortir le lien qui existe entre les deux théories.

THÉORÈME I. — *Les racines communes à deux congruences binômes de module premier p,*

$$x^m \equiv 1 \pmod{p}, \quad x^n \equiv 1 \pmod{p},$$

sont également racines de la congruence

$$x^\theta \equiv 1 \pmod{p},$$

θ étant le plus grand commun diviseur de m et de n.

$x^\theta - 1$ est, en effet, le plus grand commun diviseur de $x^m - 1$ et de $x^n - 1$. Ce théorème est, par suite, une conséquence du corollaire démontré au n° 300.

Il est évident que, réciproquement, chaque racine de la congruence $x^\theta - 1 \equiv 1$ satisfait aux deux proposées.

COROLLAIRE. — *Si θ désigne le plus grand commun diviseur des nombres m et $p - 1$, la congruence binôme du module premier,*

$$x^m \equiv 1 \pmod{p},$$

aura θ racines qui appartiendront à la congruence

$$x^\theta \equiv 1 \pmod{p}.$$

En effet, les racines de la congruence proposée appartiennent aussi à la congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

D'ailleurs, la congruence

$$x^\theta - 1 \equiv 0 \pmod{p}$$

a θ racines (n° 299), puisque son premier membre est un diviseur de $x^{p-1} - 1$; la proposée a donc elle-même θ racines.

Si m est premier avec $p-1$, on a $\theta = 1$, et dans ce cas la congruence $x^m \equiv 1$ n'a pas d'autre racine que l'unité.

D'après ce qui précède, on peut borner l'étude des congruences binômes de la forme

$$x^m \equiv 1 \pmod{p}$$

à celles dont le degré m est un diviseur de $p-1$.

Théorème II. — *Si a désigne une racine quelconque de la congruence de module premier*

$$x^m \equiv 1 \pmod{p},$$

dont le degré m est un diviseur de $p-1$, toute puissance de a ou son résidu minimum est également racine.

La congruence

$$a^m \equiv 1 \pmod{p}$$

entraîne en effet

$$a^{mk} \equiv 1 \quad \text{ou} \quad (a^k)^m \equiv 1,$$

et si b désigne le résidu minimum de a^k, par rapport à p, on a

$$a^k \equiv b, \quad \text{d'où} \quad b^m \equiv 1;$$

par conséquent, tous les termes de la série

$$a, \; a^2, \; a^3, \; \ldots,$$

ou leurs résidus minima, sont racines de la même congruence. Or, à cause de $a^m \equiv 1$, on a aussi

$$a^{m+1} \equiv a, \quad a^{m+2} \equiv a^2, \; \ldots.$$

La série précédente contient donc au plus m termes ayant des résidus différents, et ces résidus se reproduisent périodiquement de m en m. Si les m premiers termes

$$a, \; a^2, \; a^3, \; \ldots, \; a^{m-1}, \quad a^m \quad \text{ou} \quad 1$$

sont incongrus suivant le module p, leurs résidus sont les m racines de la congruence proposée. Dans le cas contraire, si l'on a, par exemple,

$$a^{n+n'} \equiv a^{n'} \pmod{p},$$

a étant premier avec p, il vient, en divisant par $a^{n'}$,

$$a^n \equiv 1 \pmod{p};$$

par conséquent, a est racine d'une congruence binôme

$$x^n \equiv 1 \pmod{p}$$

de degré n inférieur à m. De là résulte cette proposition :

Théorème III. — *Si a est une racine de la congruence $x^m \equiv 1 \pmod{p}$, qui n'appartienne à aucune congruence de degré moindre $x^n \equiv 1 \pmod{p}$, les m racines de la proposée seront les résidus des m puissances de a*

$$a,\ a^2,\ a^3,\ \ldots,\ a^{m-1},\ a^m.$$

L'analogie de la théorie que nous exposons avec celle des équations binômes conduit naturellement à appliquer la dénomination de *racines primitives* d'une congruence binôme

$$x^m \equiv 1 \pmod{p},$$

dont le degré m divise $p - 1$, à celles des racines de cette congruence qui n'appartiennent à aucune congruence de même forme et de degré moindre. Comme dans le cas des équations binômes, chaque racine primitive jouit de la propriété de donner toutes les autres racines par ses diverses puissances.

Il faut remarquer que, chaque racine non primitive de la congruence $x^m \equiv 1 \pmod{p}$ appartenant à une congruence de même forme et de degré moindre, elle ap-

partient aussi à une troisième congruence de même forme, et dont le degré divise celui de la proposée.

309. Voici maintenant comment on peut établir l'existence des racines primitives.

Considérons la congruence

(1) $$x^m \equiv 1 \pmod{p},$$

et supposons d'abord que m ne contienne qu'un seul facteur premier q, que l'on ait

$$m = q^\mu;$$

toute racine non primitive de

(2) $$x^{q^\mu} \equiv 1 \pmod{p}$$

appartient à une congruence

$$x^\theta \equiv 1 \pmod{p},$$

dont le degré θ est un diviseur de q^μ et même de $q^{\mu-1}$; et, par conséquent, cette racine appartient aussi à la congruence

(3) $$x^{q^{\mu-1}} \equiv 1 \pmod{p}.$$

D'ailleurs les racines de (3) sont aussi racines de (2); leur nombre est $q^{\mu-1}$, par conséquent celui des racines primitives de la proposée est

$$q^\mu - q^{\mu-1} \quad \text{ou} \quad q^\mu\left(1 - \frac{1}{q}\right).$$

Supposons maintenant m quelconque, et soit

$$m = q^\mu r^\nu \ldots s^\lambda,$$

$q, r, \ldots, s$ désignant des facteurs premiers inégaux.

Considérons les congruences

(4) $$x^{q^\mu} \equiv 1 \pmod{p}, \quad x^{r^\nu} \equiv 1 \pmod{p}, \ldots, \quad x^{s^\lambda} \equiv 1 \pmod{p},$$

et désignons par a une racine primitive de la première, par b une de la deuxième, etc., par l une de la dernière. Il résulte du théorème démontré au n° 307 que le résidu du produit

$$ab\ldots l$$

est une racine primitive de la proposée

$$(5)\qquad x^{q^\mu r^\nu \ldots s^\lambda} \equiv 1 \pmod{p}.$$

Mais on peut aussi établir ce point de la manière suivante : il est d'abord évident que $ab\ldots l$, ou son résidu, est racine; car on a

$$a^{q^\mu} \equiv 1,\quad b^{r^\nu} \equiv 1,\quad l^{s^\lambda} \equiv 1 \pmod{p},$$

et, par suite,

$$(ab\ldots l)^{q^\mu r^\nu \ldots s^\lambda} \equiv 1 \pmod{p}.$$

Maintenant, si ce produit n'est pas une racine primitive de la proposée, il sera racine d'une congruence

$$x^\theta \equiv 1 \pmod{p},$$

dont le degré θ sera un diviseur de m, et il y aura au moins un facteur premier de m, qui entrera dans θ moins de fois que dans m. Admettons que le facteur q soit dans ce cas; alors θ divisera $q^{\mu-1} r^\nu \ldots s^\lambda$, et, par suite, $ab\ldots l$ sera racine de la congruence

$$x^{q^{\mu-1} r^\nu \ldots s^\lambda} \equiv 1 \pmod{p};$$

on aura donc

$$(ab\ldots l)^{q^{\mu-1} r^\nu \ldots s^\lambda} \equiv 1 \pmod{p};$$

mais on a aussi

$$(b\ldots l)^{q^{\mu-1} r^\nu \ldots s^\lambda} \equiv 1 \pmod{p},$$

et, par la division,

$$a^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1 \pmod{p}.$$

On voit par là que a est racine des deux congruences

$$x^{q^{\mu-1}r^{\nu}\ldots s^{\lambda}} \equiv 1 \quad \text{et} \quad x^{q^{\mu}} \equiv 1 \pmod{p}$$

et, par suite, de

$$x^{q^{\mu-1}} \equiv 1 \pmod{p},$$

puisque $q^{\mu-1}$ est le plus grand commun diviseur entre les degrés des précédentes; a n'est donc pas, comme on l'a supposé, une racine primitive de $x^{q^{\mu}} \equiv 1 \pmod{p}$.

Il est ainsi démontré que, si $a, b, \ldots, c$ désignent des racines primitives respectivement de la première, de la deuxième, etc., de la dernière des congruences (4), le produit $ab\ldots c$, ou son résidu, est une racine primitive de la congruence proposée (5). En outre, en répétant ici le raisonnement dont nous avons fait usage au n° 104, à l'occasion de l'équation binôme, on prouvera que toutes les racines, tant primitives que non primitives, de la congruence (5), sont représentées par la formule

$$ab\ldots l,$$

où l'on doit prendre pour $a, b, \ldots, l$ toutes les racines respectivement de la première des congruences (4), de la deuxième, etc., de la dernière; et que la même formule donne toutes les racines primitives, en prenant pour $a, b, \ldots, l$ les diverses racines primitives des congruences auxquelles elles appartiennent. Comme le nombre des racines primitives a est $q^{\mu}\left(1-\frac{1}{q}\right)$, que celui des racines b est $r^{\nu}\left(1-\frac{1}{r}\right), \ldots,$ celui des racines l, $s^{\lambda}\left(1-\frac{1}{s}\right)$, on

en conclura que le nombre des racines primitives de la proposée est

$$m\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{1}{s}\right)=\varphi(m),$$

ce qui est le résultat déjà obtenu.

Théorème relatif aux résidus des puissances dont le degré est un diviseur de $p-1$.

310. Théorème. — *Le module p étant supposé premier et θ étant un diviseur de $p-1$, soient x_1 et ξ deux nombres compris entre zéro et p; si l'on a*

$$x_1^\theta \equiv \xi \pmod{p},$$

on a aussi

$$\xi^{\frac{p-1}{\theta}} \equiv 1 \pmod{p};$$

et, réciproquement, si l'on a

$$\xi^{\frac{p-1}{\theta}} \equiv 1 \pmod{p},$$

la congruence

$$x^\theta \equiv \xi \pmod{p}$$

a θ racines.

La première partie du théorème est évidente; car, si l'on a

$$x_1^\theta \equiv \xi \pmod{p},$$

en élevant les deux membres à la puissance $\frac{p-1}{\theta}$, on a

$$x_1^{p-1} \equiv \xi^{\frac{p-1}{\theta}} \pmod{p},$$

et, à cause du théorème de Fermat,

$$\xi^{\frac{p-1}{\theta}} \equiv 1 \pmod{p}.$$

Réciproquement, supposons que l'on ait $\xi^{\frac{p-1}{\theta}} \equiv 1$, ou

$$\xi^{\frac{p-1}{\theta}} - 1 = pQ;$$

retranchant chaque membre de cette égalité de $x^{p-1} - 1$, il vient

$$x^{p-1} - 1 - pQ = x^{p-1} - \xi^{\frac{p-1}{\theta}} = (x^\theta)^{\frac{p-1}{\theta}} - \xi^{\frac{p-1}{\theta}}.$$

Or le second membre admet pour diviseur $x^\theta - \xi$; il en est donc de même du premier membre $x^{p-1} - 1 - pQ$, et par conséquent, en vertu du théorème démontré au n° **299**, la congruence

$$x^\theta - \xi \equiv 0 \pmod{p}$$

a θ racines. Ce qu'il fallait démontrer.

Corollaire. — *Si p est un nombre premier, et qu'en décomposant $p - 1$ en facteurs premiers on ait trouvé*

$$p - 1 = 2^\varrho q^\mu r^\nu \ldots s^\lambda,$$

les racines non primitives de la congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p},$$

racines qui appartiennent toutes à l'une au moins des congruences

$$x^{\frac{p-1}{2}} \equiv 1, \quad x^{\frac{p-1}{q}} \equiv 1, \quad x^{\frac{p-1}{r}} \equiv 1, \quad \ldots, \quad x^{\frac{p-1}{s}} \equiv 1,$$

sont des résidus de carrés, ou de puissances q, ou de puissances r, etc., ou de puissances s; et, réciproquement, tout nombre résidu d'un carré, ou d'une puissance q, ou etc., est racine de l'une des congruences précédentes et n'est pas racine primitive du nombre premier p.

Ce corollaire résulte immédiatement du théorème qui

précède; on peut ajouter que, parmi les nombres

$$1, 2, 3, \ldots, p-1,$$

il y en a la moitié qui sont des carrés (résidus de carrés), la $q^{\text{ième}}$ partie qui sont des puissances q, la $r^{\text{ième}}$ partie des puissances $r, \ldots$, la $s^{\text{ième}}$ partie des puissances s; et, plus généralement, si l'on ne considère parmi ces nombres que ceux qui sont à la fois des puissances $2, q, r, \ldots$, la $s^{\text{ième}}$ partie de ces derniers sera en même temps des puissances s. En effet, les nombres qui sont à la fois des résidus de carrés, de puissances q, de puissances $r, \ldots$, satisfont aux congruences

$$x^{\frac{p-1}{2}} \equiv 1, \quad x^{\frac{p-1}{q}} \equiv 1, \quad x^{\frac{p-1}{r}} \equiv 1, \quad \ldots \quad (\text{mod.}\, p)$$

et, par conséquent, sont racines de

$$x^{\frac{p-1}{2qr\ldots}} \equiv 1 \quad (\text{mod.}\, p):$$

leur nombre est donc $\frac{p-1}{2qr\ldots}$; pareillement, le nombre de ceux qui sont en même temps des puissances s est $\frac{p-1}{2qr\ldots s}$: il est donc la $s^{\text{ième}}$ partie du premier.

311. La congruence

$$(1) \qquad x^{p-1} - 1 \equiv 0 \quad (\text{mod.}\, p)$$

peut se mettre sous la forme

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \quad (\text{mod.}\, p),$$

et chacune des deux congruences

$$(2) \qquad x^{\frac{p-1}{2}} - 1 \equiv 0 \; (\text{mod.}\, p),$$

$$(3) \qquad x^{\frac{p-1}{2}} + 1 \equiv 0 \quad (\text{mod.}\, p),$$

dans lesquelles elle se décompose, a $\frac{p-1}{2}$ racines. En outre, d'après le théorème du n° 310, chaque racine de la congruence (2) est un résidu de carré, ou un *résidu quadratique;* au contraire, aucune des racines de l'équation (3) ne peut être le résidu d'un carré, et ces racines sont dites *non-résidus quadratiques*, ou simplement *non-résidus.*

Le nombre a sera donc résidu ou non-résidu quadratique, relativement au module premier p, suivant qu'il satisfera à la congruence (2) ou à la congruence (3), c'est-à-dire suivant que la division de $a^{\frac{p-1}{2}}$ par p donnera le reste $+1$ ou le reste -1. Legendre a proposé de représenter ce reste par le symbole $\left(\frac{a}{p}\right)$, en sorte que l'on a

$$\left(\frac{a}{p}\right) = +1,$$

quand a est résidu quadratique, et

$$\left(\frac{a}{p}\right) = -1,$$

quand a est non-résidu.

Il est évident que, si p est de la forme $4i+1$, les deux nombres a et $-a$ sont en même temps résidus ou non-résidus. Au contraire, si p est de la forme $4i+3$, l'un des deux nombres a, $-a$ est résidu, tandis que l'autre est non-résidu.

Si les nombres a et b sont tous deux résidus ou tous deux non-résidus, on a

$$a^{\frac{p-1}{2}} \equiv \pm 1, \quad b^{\frac{p-1}{2}} \equiv \pm 1, \quad \text{d'où} \quad (ab)^{\frac{p-1}{2}} \equiv +1 \quad (\text{mod.}\, p):$$

par conséquent, le produit ab est résidu. Si, au contraire,

l'un des nombres a et b est résidu, et que l'autre soit non-résidu, on a

$$a^{\frac{p-1}{2}} \equiv \pm 1, \quad b^{\frac{p-1}{2}} \equiv \mp 1, \quad \text{d'où} \quad (ab)^{\frac{p-1}{2}} \equiv -1 \pmod{p}:$$

le produit ab est donc non-résidu.

On exprime ce résultat par la formule

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

et il est évident qu'on aura généralement

$$\left(\frac{abcd\ldots}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\left(\frac{d}{p}\right)\cdots$$

On trouvera plus loin un beau théorème de Legendre qui permet de déterminer très-facilement le signe des expressions $\left(\frac{a}{p}\right)$.

Recherche des racines primitives d'un nombre premier.

312. Le théorème du n° 310 fournit un moyen de trouver les racines primitives d'un nombre premier.

Soient p un nombre premier ; $2, q, r, \ldots, s$ les facteurs premiers inégaux de $p-1$, et écrivons les $p-1$ nombres

$$1, 2, 3, 4, \ldots, p-1;$$

si l'on enlève de cette suite tous les résidus de carrés, de puissances q, de puissances r, etc., il ne restera plus que les racines primitives de p.

Au moyen des carrés, on exclut d'abord la moitié des nombres ; au moyen des puissances q, on exclura la $q^{\text{ième}}$ partie de ceux qui restent, et ainsi de suite.

Supposons, par exemple, qu'il s'agisse de trouver les racines primitives de 31.

Écrivons les trente nombres

$$(1)\quad \left\{\begin{array}{cccccccccc} 1, & 2, & 3, & 4, & 5, & 6, & 7, & 8, & 9, & 10, \\ 11, & 12, & 13, & 14, & 15, & 16, & 17, & 18, & 19, & 20, \\ 21, & 22, & 23, & 24, & 25, & 26, & 27, & 28, & 29, & 30; \end{array}\right.$$

comme les facteurs premiers de 30 sont 2, 3 et 5, il suffira d'enlever de la suite (1) les résidus des carrés, des cubes et des cinquièmes puissances.

Pour exclure les carrés, nous élèverons les nombres (1) au carré; les carrés des quinze premiers sont

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225,

et ils ont pour résidus

(2) 1, 4, 9, 16, 25, 5, 18, 2, 19, 7, 28, 20, 14, 10, 8;

les carrés des quinze derniers nombres de la suite (1) donneraient les mêmes racines, car on a

$$(31 - h)^2 \equiv h^2 \quad (\text{mod. } 31).$$

Otant ces quinze nombres (2) de la suite (1), il restera les quinze que voici :

(3) 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, 24, 26, 27, 29, 30,

dont il faut maintenant supprimer les cubes et les cinquièmes puissances. Chaque nombre déjà supprimé (2) satisfait à la congruence

$$x^{15} \equiv 1 \quad (\text{mod. } 31);$$

donc sa puissance troisième et sa puissance cinquième y satisfont aussi, et, par conséquent, font partie des nombres déjà supprimés. D'après cela, les nombres de la suite (3) qu'il reste à rejeter sont des résidus de puissances troisième et cinquième de ces mêmes nombres (3). Pour avoir les résidus des cubes de la suite (3), il suffit de multiplier les premières puissances par les résidus

quadratiques que la suite (2) fait connaître et qui sont

9, 5, 28, 20, 14, 8, 10, 7, 19, 2, 18, 25, 16, 4, 1;

on aura ainsi les résidus cubiques suivants :

27, 30, 308, 240, 182, 120, 170, 147, 418, 46, 432, 650, 432, 116, 30,

dont les résidus minima sont

(4) 27, 30, 29, 23, 27, 27, 15, 23, 15, 15, 29, 30, 29, 23, 30.

Il n'y en a que cinq de différents, comme nous le savions d'avance ; ce sont

(5) 15, 23, 27, 29, 30,

et en ôtant ces nombres de la suite (3), il ne restera plus que les dix suivants :

(6) 3, 6, 11, 12, 13, 17, 21, 22, 24, 26,

dont il n'y a plus à rejeter que ceux qui sont des cinquièmes puissances. Chacun des nombres déjà exclus satisfait à l'une des congruences

$$x^{15} \equiv 1 \pmod{31}, \quad x^{10} \equiv 1 \pmod{31}.$$

Il en est donc de même de sa cinquième puissance, qui, par conséquent, fait partie des nombres exclus : un nombre de la suite (6) ne peut donc être la cinquième puissance que d'un nombre de la même suite. Pour avoir les résidus des cinquièmes puissances des nombres (6), il suffit de multiplier les résidus cubiques déjà formés par les résidus quadratiques correspondants, et de prendre les résidus minima des produits. Les résidus cubiques sont

27, 30, 29, 23, 27, 15, 23, 15, 29, 30,

les quadratiques

9, 5, 28, 20, 14, 10, 7, 19, 18, 25;

les produits sont

243, 150, 812, 460, 378, 150, 161, 285, 522, 750,

et l'on trouve pour résidus des cinquièmes puissances

26, 26, 6, 26, 6, 26, 6, 6, 26, 6.

Il n'y a ainsi, dans la suite (6), que deux cinquièmes puissances, comme nous le savions déjà, savoir :

6, 26;

en supprimant ces deux nombres, il ne restera plus que les huit racines primitives de 31, savoir :

3, 11, 12, 13, 17, 21, 22, 24.

313. La recherche des racines primitives ne peut guère s'effectuer que par tâtonnements; le procédé que nous venons d'indiquer est presque impraticable dès que le module est un peu considérable; aussi croyons-nous utile de faire connaître une autre méthode due à Gauss, et par laquelle on peut obtenir assez facilement une racine primitive; les autres racines primitives pourront être déterminées ensuite, comme nous l'avons indiqué précédemment (n° 306).

On prendra arbitrairement un nombre a dans la suite $2, 3, \ldots, (p-1)$, 2 par exemple, et l'on déterminera sa période, c'est-à-dire la période des restes fournis par les puissances

$$a,\ a^2,\ a^3,\ \ldots.$$

Si cette période a $p-1$ termes, a sera une racine primitive; mais, si la période a moins de $p-1$ termes, on prendra un autre point b qui ne soit pas compris parmi les restes de la suite (1), et l'on cherchera de même la période de b. Si cette période de b a $p-1$ termes, b sera racine primitive; mais supposons qu'il n'en soit pas

ainsi. Désignons par n l'exposant auquel a appartient, et par m celui auquel appartient b; comme les restes de la suite (1) comprennent tous les nombres qui appartiennent à l'exposant n, et, pour la même raison, ceux qui appartiennent à un exposant sous-multiple de n, le nombre m ne sera pas un diviseur de n. Mais il peut être un multiple de n, et, quand ce cas se présente, la connaissance de b aura avancé la solution de la question, car ce nombre appartient à un exposant plus élevé que celui auquel a se rapporte. Supposons que m ne soit égal ni à $p-1$ ni à un multiple de n; désignons par s le plus petit commun multiple de n et m, et décomposons ce nombre s en deux facteurs premiers entre eux n', m', qui divisent respectivement les nombres n et m. Voici comment cette décomposition peut être effectuée : on décomposera les nombres n et m en leurs facteurs premiers; soit c l'un de ces facteurs premiers destiné à entrer dans s avec l'exposant γ. Si c^γ est diviseur de n seul, on fera figurer c^γ dans n'; si c^γ est diviseur de m seul, on introduira au contraire c^γ dans m'; enfin, si c^γ est diviseur commun de m et de n, on introduira c^γ à volonté, soit dans m', soit dans n'; on agira de même à l'égard des autres facteurs premiers de s. On aura ainsi $s = n'm'$, avec $n = n'e$, $m = m'f$, e et f étant des entiers. Cela posé, je dis que le nombre a^e appartient à l'exposant n', relativement au diviseur p; en effet, la puissance $n'^{\text{ième}}$ de a^e est a^n, et elle donne en conséquence le reste 1; il n'y a pas d'ailleurs d'exposant ν inférieur à n' tel que $(a^e)^\nu$ ou $a^{\nu e}$ donne le reste 1, puisque νe est inférieur à n et que a appartient à l'exposant n. On ferait voir de même que b^f appartient à l'exposant m', et il en résulte (n° 307) que le produit $a^e . b^f$ ou le résidu de ce produit appartient à l'exposant $m'n' = s$.

La méthode que nous venons d'exposer conduit, dans tous les cas, à un nombre qui appartient à un exposant

plus élevé que celui auquel appartient le nombre a duquel on est parti. En poursuivant la même marche, on arrivera donc certainement à un nombre appartenant à l'exposant $p-1$; ce nombre sera une racine primitive de p. Mais, dans la plupart des cas, il se présente des circonstances particulières qui permettent de simplifier l'application de la méthode.

314. Premier exemple. — *On demande une racine primitive du nombre premier* 71.

Prenons le nombre 2 et cherchons sa période. A cet effet, on formera la série des puissances de 2; chacune d'elles s'obtient en multipliant la puissance précédente par 2; mais, avant de faire cette multiplication, il faut avoir soin de retrancher 71 de la puissance qui sert de multiplicande, lorsque celle-ci est supérieure à 71. On trouve que la période de 2 a 35 termes qui sont

$$(1)\quad \left\{\begin{array}{rrrrrrr} 2, & 4, & 8, & 16, & 32, & 64, & 57, \\ 43, & 15, & 30, & 60, & 49, & 27, & 54, \\ 37, & 3, & 6, & 12, & 24, & 48, & 25, \\ 50, & 29, & 58, & 45, & 19, & 38, & 5, \\ 10, & 20, & 40, & 9, & 18, & 36, & 1. \end{array}\right.$$

Le nombre 2 n'est donc pas racine primitive de 71, et il appartient à l'exposant 35; mais il est facile de voir que le complément de 2 à 71, c'est-à-dire 69, est racine primitive. En effet, de l'identité

$$69 = 71 - 2,$$

on tire

$$\left.\begin{array}{l} 69^2 \equiv 2^2 \\ 69^3 \equiv -2^3 \end{array}\right\} \pmod{71},$$

d'où il résulte que la suite des restes fournis par les puissances de 69 pourra se déduire de la suite des restes des

puissances de 2; il suffira effectivement de remplacer, dans cette dernière suite, les restes de rang impair par leurs compléments à 71, sans rien changer aux restes de rang pair. Dans la suite des restes fournis par les puissances de (2) et dont la première période est l'ensemble des nombres (1), le reste 1 occupe les rangs 35, 70, ...; ce reste 1 n'apparaîtra donc qu'au 70e rang, dans la période de 69, et en conséquence 69 est racine primitive. Formons la période de 69 en suivant la marche que nous venons d'indiquer, c'est-à-dire en prenant deux fois la période (1) du nombre 2 et en remplaçant les termes de rang impair par leurs compléments à 71, on trouvera:

(2)

69,	4,	63,	16,	39,	64,	14,
43,	56,	30,	11,	49,	44,	54,
34,	3,	65,	12,	47,	48,	46,
50,	42,	58,	26,	19,	33,	5,
61,	20,	31,	9,	53,	36,	70,
2,	67,	8,	55,	32,	7,	57,
28,	15,	41,	60,	22,	27,	17,
37,	68,	6,	59,	24,	23,	25,
21,	29,	13,	45,	52,	38,	66,
10,	51,	40,	62,	18,	35,	1,

et ceux des nombres du tableau (2) dont les rangs sont marqués par des nombres premiers à 70 seront les racines primitives de 71. Les 24 racines primitives de 71, dans l'ordre où elles se présentent comme restes de puissances de 69, sont ainsi

69, 63, 56, 11, 44, 65, 47, 42,
33, 61, 31, 53, 67, 55, 7, 28,
22, 68, 59, 21, 13, 52, 62, 35;

la plus petite de ces racines primitives est 7.

315. SECOND EXEMPLE. — *On demande une racine primitive du nombre premier 73.*

On formera, comme précédemment, la période du nombre 2; on trouve ici que cette période n'a que 9 termes et qu'elle se compose des nombres

2, 4, 8, 16, 32, 64, 55, 37, 1;

le nombre 2 appartient donc à l'exposant 9, relativement à 73. Comme 3 ne fait pas partie de la suite précédente, nous formerons de même la période de 3; celle-ci se compose des 12 termes suivants:

3, 9, 27, 8, 24, 72,
70, 64, 46, 65, 49, 1;

en sorte que 3 appartient à l'exposant 12. Le plus petit multiple commun des nombres 9 et 12 étant 36, la méthode du n° 307 fera connaître un nombre appartenant à l'exposant 36. Cet exposant 36 est le produit des facteurs 9 et 4 qui sont premiers entre eux et qui divisent respectivement 9 et 12; les quotients de ces divisions sont 1 et 3; par conséquent le nombre 2×3^3 ou 54 appartient à l'exposant 36. Formons la période de 54, on trouve les 36 termes suivants :

54,	69,	3,	16,	61,	9,	48,	37,	27,
71,	38,	8,	67,	41,	24,	55,	50,	72,
19,	4,	70,	57,	12,	64,	25,	36,	46,
2,	35,	65,	6,	32,	49,	18,	23,	1,

qu'on obtient très-facilement en remarquant qu'un terme quelconque se forme en multipliant par 3 celui qui le précède de 3 rangs et en prenant le résidu du produit obtenu, relativement à 73; cela résulte de ce que 3 est le cube de 54 diminué d'un multiple de 73. Maintenant le nombre 5 ne fait pas partie du tableau précédent, mais

son carré 5^2 ou 25 s'y trouve et il y occupe un rang marqué par le nombre 25 qui est premier à 72. Il résulte de là que 5^2 appartient à l'exposant 36; l'exposant auquel 5 appartient est donc égal à 36×2 ou à 72; en d'autres termes, 5 est une racine primitive de 73.

316. Nous donnons ici une Table dans laquelle on trouve la plus petite racine primitive pour chacun des nombres premiers inférieurs à 100.

Nombres premiers.	3	5	7	11	13	17	19	23	29	31	37	41
Racines primitives.	2	2	3	2	2	3	2	5	2	3	2	6

Nombres premiers.	43	47	53	59	61	67	71	73	79	83	89	97
Racines primitives.	3	5	2	2	2	2	7	5	3	2	3	5

Et à cette occasion nous présenterons les remarques suivantes :

1° Si p est de la forme $4k+1$ et que a soit racine primitive, $-a$ est aussi racine primitive.

2° Si p est de la forme $4k+3$, a et $-a$ ne peuvent être en même temps racines primitives.

En effet, tout nombre qui n'est pas racine primitive, par rapport à p, satisfait à une congruence telle que

$$x^{\frac{p-1}{\theta}} \equiv 1 \quad (\text{mod.} \, p),$$

θ étant un diviseur premier de $p-1$. Lorsque $p = 4k+1$, $\frac{p-1}{\theta}$ est un nombre pair, et les racines de la précédente congruence sont, deux à deux, égales et de signes contraires, ou complémentaires au module. En

second lieu, lorsque $p = 4k + 3$, si a satisfait à la congruence $x^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, le nombre $-a$ satisfait à $x^{\frac{p-1}{2}} = \mp 1 \pmod{p}$; donc l'un au moins des nombres a et $-a$ n'est pas racine primitive.

Des racines primitives dans le cas où le module est égal à une puissance d'un nombre premier impair, ou égal au double d'une telle puissance.

317. Théorème I. — *Si p est un nombre premier impair, et que g soit une racine primitive pour le module p^ν, g ou son résidu minimum, relativement à p, sera également racine primitive pour le module p.*

En effet, désignons par n l'exposant auquel appartient g, relativement à p, on aura

$$g^n \equiv 1 \pmod{p},$$

ou

$$g^n = 1 + kp,$$

k étant un entier. En élevant cette égalité à la puissance p, il vient

$$g^{np} = 1 + \frac{p}{1} kp + \frac{p(p-1)}{1.2} k^2 p^2 + \ldots;$$

dans le second membre de cette formule, tous les termes, à l'exception du premier, sont divisibles par p^2; on a donc

$$g^{np} = 1 + k_1 p^2,$$

k_1 étant un nombre entier. On trouvera de même, par des élévations successives à la puissance p,

$$g^{np^2} = 1 + k_2 p^3,$$

$$\ldots\ldots\ldots\ldots\ldots,$$

$$g^{np^{\nu-1}} = 1 + k_{\nu-1} p^\nu,$$

k_2, ... $k_{\nu-1}$ étant des entiers. La dernière de ces égalités peut être mise sous la forme

$$g^{np^{\nu-1}} \equiv 1 \pmod{p^\nu},$$

et elle montre que g ne peut être racine primitive, pour le module p^ν, que si $n = p - 1$, et, dans ce cas, g est racine primitive de p.

318. Théorème II. — *Une racine primitive g du module premier impair p est racine primitive pour le module p^ν, ν étant > 1, lorsque $\frac{g^{p-1}-1}{p}$ n'est pas divisible par p. Au contraire, g n'est pas racine primitive pour le module p^ν, quand $\frac{g^{p-1}-1}{p}$ est divisible par p.*

En effet, désignons par t l'exposant auquel g appartient relativement au module p^ν; on aura

$$g^t \equiv 1 \pmod{p^\nu},$$

et par conséquent

$$g^t \equiv 1 \pmod{p}.$$

Comme g est, par hypothèse, racine primitive de p, la congruence précédente exige que t soit un multiple de $p-1$; d'ailleurs t est un diviseur de

$$\varphi(p^\nu) = p^{\nu-1}(p-1);$$

donc on a

$$t = p^\lambda(p-1),$$

λ étant un nombre inférieur ou égal à $\nu - 1$.

Cela posé, désignons par i l'exposant de la plus haute puissance de p qui divise $g^{p-1} - 1$, on aura

$$g^{p-1} = 1 + kp^i,$$

k étant un entier non divisible par p; on a ensuite, comme au numéro précédent, par des élévations succes-

sives à la puissance p, et en remarquant que i ne peut être nul,

$$g^{p(p-1)} = 1 + k_1 p^{i+1},$$
$$g^{p^2(p-1)} = 1 + k_2 p^{i+2},$$
$$\ldots\ldots\ldots\ldots\ldots,$$
$$g^{p^\lambda(p-1)} = 1 + k_\lambda p^{i+\lambda},$$

$k_1, k_2, \ldots, k_\lambda$ étant des entiers non divisibles par p.

On voit, par ces formules, que la plus petite des valeurs de λ telles, que l'on ait

$$g^{p^\lambda(p-1)} \equiv 1 \pmod{p^\nu},$$

est

$$\lambda = \nu - i.$$

Donc on a

$$\lambda = \nu - 1$$

si $i = 1$, et

$$\lambda < \nu - 1$$

si i est > 1.

Dans le premier cas, g appartient à l'exposant $\varphi(p^\nu)$, relativement à p^ν; en d'autres termes, g est une racine primitive. Dans le second cas, g appartient à un exposant inférieur à $\varphi(p^\nu)$, et il n'est pas en conséquence racine primitive.

319. Théorème III. — *A chaque racine primitive pour le nombre premier p correspondent $p^{\nu-2}(p-1)$ racines primitives pour le module p^ν.*

Soit a une racine primitive de p, prise entre zéro et $p-1$; l'expression des racines primitives congrues à a sera

$$g = a + kp,$$

k étant un entier quelconque; on tire de là

$$g^{p-1} - 1 = (a^{p-1} - 1) + \frac{p-1}{1} a^{p-2} kp + \frac{(p-1)(p-2)}{1.2} a^{p-3} k^2 p^2 + \ldots$$

Supposons d'abord que $a^{p-1}-1$ ne soit pas divisible par p^2 : $g^{p-1}-1$ sera divisible ou non divisible par p^2, suivant que

$$\frac{a^{p-1}-1}{p} + (p-1)a^{p-2}k$$

ou

$$\frac{a^p-a}{p} - k$$

sera divisible ou non divisible par p. Si donc on désigne par α le résidu minimum de $\frac{a^p-a}{p}$ par rapport à p, et que l'on fasse

$$k = \alpha + h,$$

h étant un nombre non divisible par p, tous les nombres g compris dans la formule

$$(1) \qquad g = a + (\alpha + h)p$$

seront, d'après le théorème II, des racines primitives pour le module p^ν.

Supposons en second lieu que $a^{p-1}-1$ soit divisible par p^2 ; dans ce cas, $g^{p-1}-1$ ne sera divisible par p^2 que si k est divisible par p : d'où il résulte que la formule

$$(2) \qquad g = a + hp,$$

où h désigne un nombre non divisible par p, ne donnera que des racines primitives de p^ν.

Si l'on ne veut avoir que les valeurs de g distinctes suivant le module p^ν, on ne devra donner à h dans les formules (1) et (2) que $\varphi(p^{\nu-1}) = p^{\nu-2}(p-1)$ valeurs différentes, et il en résultera un pareil nombre de racines primitives pour le module p^ν.

Remarque. — Comme a est racine primitive de p, le nombre $a^{p-1}-1 = \left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)$ ne peut être

divisible par p^2 que si l'on a

$$a^{\frac{p-1}{2}}+1 \equiv 0 \pmod{p^2}.$$

Corollaire. — *Le nombre des racines primitives, pour le module p^ν, est égal à $\varphi[p^{\nu-1}(p-1)]$ ou à $\varphi\varphi(p^\nu)$.*

En effet, d'après le théorème I, chaque racine primitive de p^ν est racine primitive de p; d'ailleurs, d'après le précédent théorème, chacune des $\varphi(p-1)$ racines primitives de p donne $\varphi(p^{\nu-1})$ racines primitives de p^ν. Le nombre total de ces dernières est donc

$$\varphi(p^{\nu-1})\varphi(p-1) = \varphi[p^{\nu-1}(p-1)] = \varphi\varphi(p^\nu).$$

320. Théorème IV. — *Le nombre premier p étant impair, toute racine primitive impaire de p^ν est en même temps racine primitive pour le module $2p^\nu$; et réciproquement, toute racine primitive de $2p^\nu$ est racine primitive pour le module p^ν.*

Soit g un nombre impair non divisible par p, et désignons par n, n' les exposants auxquels g appartient relativement aux modules respectifs p^ν, $2p^\nu$; on aura

$$(1) \qquad g^n \equiv 1 \pmod{p^\nu}, \qquad g^{n'} \equiv 1 \pmod{2p^\nu}.$$

La seconde de ces congruences donne

$$(2) \qquad g^{n'} \equiv 1 \pmod{p^\nu}$$

et, par conséquent, n' est un multiple de n. En outre, g étant impair, on a $g^n \equiv 1 \pmod{2}$; par conséquent, la première des congruences (1) donne aussi

$$g^n \equiv 1 \pmod{2p^\nu},$$

d'où il suit que n est un multiple de n'. On a donc $n = n'$,

et le nombre g appartient au même exposant suivant les modules p^ν, $2p^\nu$.

Enfin, comme on a

$$\varphi(2p^\nu) = \varphi(p^\nu) = p^{\nu-1}(p-1),$$

si le nombre g est racine primitive pour l'un des modules, il l'est aussi pour l'autre.

Corollaire. — *Il y a autant de racines primitives pour le module $2p^\nu$ que pour le module p^ν.*

En effet, si l'on prend les racines primitives impaires de p^ν et qu'on leur adjoigne les racines primitives paires augmentées chacune de p^ν, on obtiendra $\varphi\varphi(p^\nu)$ racines primitives de $2p^\nu$.

321. Exemple. — Considérons le cas de $p = 7$. Les racines primitives de 7 sont 3 et 5 : on a

$$3^3 \equiv 27, \quad 5^3 = 125 \equiv 27 \quad (\text{mod. } 49);$$

donc 3 et 5 sont racines primitives pour les modules 7^ν et $2 \times 7^\nu$, quel que soit l'exposant ν.

Supposons $\nu = 2$, et considérons d'abord le cas du module 49. Comme on a

$$\frac{3^7 - 3}{7} = 312 \equiv 4, \quad \frac{5^7 - 5}{7} = 11160 \equiv 2 \quad (\text{mod. } 7),$$

le nombre désigné par α au n° 319 a respectivement les valeurs 4 et 2. Les racines primitives de 49 seront donc données par les formules

$$g = 3 + 7(h + 4), \quad g = 5 + 7(h + 2),$$

où h est premier avec 7; en donnant à cette indéterminée les valeurs

$$-4, \ -3, \ -2, \ -1, \ +1, \ +2$$

dans la première formule, et les valeurs

$$-2,\quad -1,\quad +1,\quad +2,\quad +3,\quad +4$$

dans la seconde, on obtient les deux séries suivantes, composées chacune de six racines :

$$3,\quad 10,\quad 17,\quad 24,\quad 38,\quad 45,$$
$$5,\quad 12,\quad 26,\quad 33,\quad 40,\quad 47,$$

ou

$$3,\quad 3^{13},\quad 3^{25},\quad 3^{37},\quad 3^{19},\quad 3^{31},$$
$$3^{29},\quad 3^{11},\quad 3^{17},\quad 3^{41},\quad 3^{23},\quad 3^{5}.$$

Quant au module 2×49 ou 98, ses douze racines primitives seront

$$3,\quad 17,\quad 45,\quad 59,\quad 73,\quad 87,$$
$$5,\quad 33,\quad 47,\quad 61,\quad 75,\quad 89.$$

De la congruence $x^t - 1 \equiv 0 \pmod{\mathrm{M}}$, *dans le cas où* M *est égal à une puissance d'un nombre premier impair ou égal au double d'une telle puissance.*

322. Le nombre p étant premier et impair, soit a une racine de la congruence

(1) $$x^t - 1 \equiv 0 \quad (\text{mod.}\, p^\nu \text{ ou } 2p^\nu),$$

on aura, à la fois,

$$a^t \equiv 1, \quad a^{p^{\nu-1}(p-1)} \equiv 1 \quad (\text{mod.}\, p^\nu \text{ ou } 2p^\nu).$$

Si donc θ désigne l'exposant auquel appartient a, relativement au module $\mathrm{M} = p^\nu$ ou $= 2p^\nu$, le nombre θ sera un diviseur commun des nombres

$$t, \quad p^{\nu-1}(p-1);$$

par suite il divisera le plus grand commun diviseur n de ces mêmes nombres. D'après cela, comme on a

$$a^\theta \equiv 1 \quad (\text{mod.}\, p^\nu \text{ ou } 2p^\nu);$$

6.

on aura aussi

$$a^n \equiv 1 \quad (\text{mod. } p^\nu \text{ ou } 2p^\nu),$$

ce qui montre que toutes les racines de la congruence proposée appartiennent aussi à la suivante :

$$(2) \qquad x^n - 1 \equiv 0 \quad (\text{mod. } p^\nu \text{ ou } 2p^\nu),$$

dont le degré n est un diviseur de $p^{\nu-1}(p-1)$.

Lorsque n est égal à $p^{\nu-1}(p-1)$, la congruence (2) devient

$$(3) \qquad x^{p^{\nu-1}(p-1)} - 1 \equiv 0 \quad (\text{mod. } p^\nu \text{ ou } 2p^\nu),$$

et nous savons qu'elle a pour racines les $p^{\nu-1}(p-1)$ nombres premiers au module et non supérieurs à ce module ; en outre, parmi ces racines, il y en a $\varphi[p^{\nu-1}(p-1)]$ de primitives, et nous avons fait connaître un procédé pour les obtenir. Si a désigne une de ces racines primitives, les résidus minima des puissances

$$(4) \qquad 1,\ a,\ a^2,\ a^3,\ \ldots,\ a^{p^{\nu-1}(p-1)}$$

seront précisément les racines de la congruence (3).

Supposons que n soit un diviseur quelconque de $p^{\nu-1}(p-1)$; posons

$$p^\nu(p-1) = n\theta,$$

et considérons un terme quelconque a^m de la suite (4). Pour que l'on ait

$$(a^m)^n \equiv 1 \quad \text{ou} \quad a^{mn} \equiv 1 \quad (\text{mod. } p^\nu \quad \text{ou} \quad 2p^\nu),$$

il faut et il suffit que mn soit divisible par $n\theta$, c'est-à-dire que m soit un multiple de θ. Donc la congruence (2) a précisément n racines qui sont les résidus des puis-

sances

$$(5) \qquad a^\theta,\ a^{2\theta},\ \ldots,\ a^{n\theta},$$

suivant le module p^ν ou $2p^\nu$. On a ainsi ce théorème :

THÉORÈME I. — *La congruence* $x^t - 1 \equiv 0$ (mod. p^ν *ou* $2p^\nu$) *a autant de racines qu'il y a d'unités dans le plus grand commun diviseur des nombres* t *et* $p^{\nu-1}(p-1)$.

Ensuite soit $a^{i\theta}$ un quelconque des termes de la suite (5). Pour que l'on ait

$$(a^{i\theta})^k \equiv 1 \quad \text{ou} \quad a^{ki\theta} \equiv 1 \quad (\text{mod. } p^\nu \quad \text{ou} \quad 2p^\nu),$$

il faut et il suffit que $ki\theta$ soit divisible par $n\theta$, ou ki par n. Si i est premier à n, cette condition équivaut à celle de la divisibilité de k par n; dans ce cas, $a^{i\theta}$ appartient évidemment à l'exposant n. Mais, si i et n ont un plus grand commun diviseur d supérieur à 1, on aura

$$(a^{i\theta})^{\frac{n}{d}} = \left(a^{\frac{i}{d}}\right)^{n\theta} \equiv 1 \quad (\text{mod. } p^\nu \text{ ou } 2p^\nu),$$

et $a^{i\theta}$ appartiendra à l'exposant $\frac{n}{d}$. On conclut de là cette autre proposition :

THÉORÈME II. — *La congruence* $x^n \equiv 1$ (mod. p^ν *ou* $2p^\nu$), *dont le degré* n *est un diviseur de* $p^{\nu-1}(p-1)$, *a autant de racines primitives, c'est-à-dire de racines qui appartiennent à l'exposant* n, *qu'il y a d'unités dans le nombre* $\varphi(n)$ *des nombres premiers et non supérieurs à* n.

Du module 2^ν.

323. On a vu, au n° 305, que si ν est > 2, la puissance de degré $2^{\nu-2}$ d'un nombre impair quelconque est congrue à l'unité, suivant le module 2^ν. Le seul cas de

$\nu = 2$ fait exception; il y a effectivement, pour le module 4, une racine primitive égale à 3, ainsi que nous l'avons déjà dit.

Supposons donc $\nu > 2$; alors l'exposant auquel appartient, relativement au module 2^ν, un nombre impair quelconque, est une puissance de 2 dont le degré est égal ou inférieur à $\nu - 2$.

Le nombre 1 est le seul qui appartienne à l'exposant 1; occupons-nous des nombres impairs supérieurs à 1. Chacun d'eux peut être représenté par la formule

$$(1) \qquad a = 2^{i+2} k \pm 1,$$

où k désigne un nombre impair et i un exposant qui peut être nul. Par des élévations successives au carré, on déduit de cette formule

$$(2) \qquad \begin{cases} a^2 = 2^{i+3} k_1 \quad + 1, \\ a^{2^2} = 2^{i+4} k_2 \quad + 1, \\ \dots\dots\dots\dots\dots\dots, \\ a^{2^\delta} = 2^{i+2+\delta} k_\delta + 1, \end{cases}$$

$k_1, k_2, \ldots, k_\delta$ étant des nombres impairs.

Supposons que 2^δ soit l'exposant auquel appartient le nombre a; on aura

$$i + 2 + \delta = \text{ ou } > \nu;$$

l'inégalité ne peut avoir lieu si δ est > 1, car autrement $a^{2^{\delta-1}} - 1$ serait divisible par 2^ν, d'après les formules (2), et l'exposant auquel a appartient serait inférieur à 2^δ. On a donc

$$i + 2 = \nu - \delta,$$

et la formule (1) devient

$$(3) \qquad a = 2^{\nu-\delta} k \pm 1.$$

On peut donner à k les $2^{\delta-1}$ valeurs

$$1,\ 3,\ 5,\ \ldots,\ (2^\delta - 1),$$

et, à cause du signe ambigu $\pm$, il en résultera, pour a, deux séries composées chacune de $2^{\delta-1}$ valeurs; on conclut de là cette proposition :

Théorème. — *Si δ désigne l'un des nombres* 2, 3, 4, ..., $(\nu - 2)$, *il y a 2^δ nombres qui appartiennent à l'exposant 2^δ suivant le module 2^ν.*

Si le nombre a déjà considéré appartient à l'exposant 2, la première des formules (2) nous donne

$$i + 3 = \text{ ou } > \nu, \quad i + 2 = \text{ ou } > \nu - 1;$$

mais, si l'on prend $i + 2 = \nu$, comme a est supposé moindre que le module 2^ν, il faut faire $k = 1$ dans la formule (1) et remplacer le signe ambigu $\pm$ par $-$; il y a donc trois nombres qui appartiennent à l'exposant 2, savoir :

$$(4) \qquad 2^{\nu-1} - 1, \quad 2^{\nu-1} + 1, \quad 2^\nu - 1.$$

Les nombres qui appartiennent à l'exposant $\nu - 2$, le plus élevé dans le cas qui nous occupe, s'obtiennent en faisant $\delta = \nu - 2$ dans la formule (3), et si l'on remplace, en même temps, k par $2k + 1$, on obtient les deux formules

$$a = 8k + 3, \quad a = 8k + 5,$$

qui donnent tous les nombres appartenant à l'exposant $2^{\nu-2}$. Cela suppose cependant que ν soit supérieur à 3; car, dans le cas de $\nu = 3$, les nombres qui appartiennent à l'exposant 2 sont, d'après les formules (4),

$$3,\ 5,\ 7.$$

Laissant ce cas de côté et supposant $\nu > 3$, désignons

par b un nombre quelconque de la forme $8k+3$ et par c un nombre quelconque de la forme $8k+5$. Chacune des deux suites

$$b,\ b^2,\ \ldots,\ b^{2^{\nu-2}},$$
$$c,\ c^2,\ \ldots,\ c^{2^{\nu-2}}$$

donnera $2^{\nu-2}$ résidus distincts, puisque b et c appartiennent à l'exposant $2^{\nu-2}$; en outre, les puissances impaires de b et de c sont respectivement des formes $8k+3$, $8k+5$, tandis que les puissances paires de l'un et de l'autre nombre sont de la forme $8k+1$; il y a d'ailleurs $2^{\nu-3}$ nombres de chacune des formes

$$8k+1,\ 8k+3,\ 8k+5,\ 8k+7$$

entre les limites 1 et $2^\nu - 1$. Donc la série des puissances de b donnera tous les nombres $8k+3$ avec les nombres $8k+1$; pareillement, on retrouvera les nombres $8k+1$ dans la série des puissances de c, avec les nombres $8k+5$.

Maintenant, si l'on change les signes des nombres $8k+1$ et $8k+5$ ou qu'on prenne leurs compléments au module 2^ν, il est évident qu'on obtiendra tous les nombres $8k+7$ et $8k+3$; on a donc la proposition suivante :

Théorème. — *Si l'on choisit un nombre quelconque de la forme* $8k+3$ *ou* $8k+5$, *qu'on prenne les résidus de ses* $2^{\nu-2}$ *premières puissances par rapport au module* 2^ν, *et qu'on joigne à ces résidus leurs compléments au module, on obtiendra la suite de tous les nombres impairs inférieurs au module.*

De la congruence $x^t - 1 \equiv 0 \pmod{2^\nu}$.

324. Considérons la congruence

$$(1)\qquad x^t - 1 \equiv 0 \pmod{2^\nu},$$

ν étant > 2. Chacune de ses racines a est telle que l'on a

$$a^t \equiv 1, \quad a^{2^{\nu-2}} \equiv 1 \pmod{2^\nu} :$$

l'exposant auquel a appartient divise donc les nombres t et $2^{\nu-2}$, ainsi que leur plus grand commun diviseur ; nous désignerons par 2^δ ce plus grand commun diviseur, et alors a sera racine de la congruence

$$(2) \qquad x^{2^\delta} - 1 \equiv 0 \pmod{2^\nu};$$

réciproquement la proposée admettra toutes les racines de la congruence (2). Il est évident que celles-ci ne sont autre chose que les nombres qui appartiennent à l'un des exposants

$$1,\ 2,\ 2^2,\ \ldots,\ 2^\delta.$$

Si t est un nombre impair, on a $\delta = 0$ et les congruences (1) et (2) n'admettent pas d'autre racine que 1. Supposons $\delta > 0$; nous avons vu que, si μ est > 1, il y a 2^μ nombres qui appartiennent à l'exposant 2^μ, et qu'il y a 3 nombres appartenant à l'exposant 2 ; le nombre des racines de la congruence (2) est donc

$$1 + 3 + 2^2 + 2^3 + \ldots + 2^\delta,$$

ou $2^{\delta+1}$. On a ainsi cette proposition :

Théorème. — *Si t est un nombre pair, le nombre des racines de la congruence $x^t - 1 \equiv 0 \pmod{2^\nu}$ est égal au double du plus grand commun diviseur des nombres t et $2^{\nu-2}$.*

Ces racines formeront deux périodes ; car désignons par c un nombre appartenant à l'exposant $2^{\nu-2}$, et posons

$$a \equiv c^{2^{\nu-2-\delta}} \pmod{2^\nu},$$

il est évident, d'après les développements qui précèdent,

que les racines des congruences (1) et (2) pourront être représentées par

$$a,\quad a^2,\quad a^3,\ \ldots,\quad a^{2\delta},$$
$$-a,\ -a^2,\ -a^3,\ \ldots,\ -a^{2\delta}.$$

De la congruence $x^t \equiv 1$, dans le cas d'un module quelconque.

325. La congruence

(1) $$x^t - 1 \equiv 0 \pmod{M},$$

dans le cas d'un module composé quelconque, se ramène facilement aux cas que nous venons de considérer.

Soit, en effet,

$$M = p^\nu q^\mu r^\lambda \ldots,$$

$p, q, r, \ldots$ étant des nombres premiers inégaux. Il est évident que toute racine de la congruence proposée doit satisfaire à la même congruence

(2) $$x^t - 1 \equiv 0,$$

suivant chacun des modules p^ν, q^μ, r^λ, ... Réciproquement, si $a, b, c, \ldots$ désignent des racines de la précédente congruence suivant les modules respectifs p^ν, q^μ, r^λ, ..., et que l'on détermine le nombre x de manière que l'on ait

$$x \equiv a \pmod{p^\nu},$$
$$x \equiv b \pmod{q^\mu},$$
$$x \equiv c \pmod{r^\lambda},$$
$$\ldots\ldots\ldots\ldots,$$

ce nombre x satisfera à la congruence (2) suivant chacun des modules p^ν, q^μ, r^λ, ..., et, par conséquent, il satisfera aussi à la même congruence prise suivant le module M.

D'après cela, la recherche des racines de la congruence proposée est ramenée à la résolution de congruences dont le module est une puissance d'un nombre premier et au problème dont nous avons donné la solution au n° 290.

Des indices.

326. L'existence des racines primitives, pour un module M égal à une puissance d'un nombre premier impair ou égal au double d'une telle puissance, entraîne des conséquences très-importantes que nous devons présenter ici.

Soit a l'une quelconque des racines primitives ; les puissances de a donneront tous les nombres premiers au module. Si donc N désigne l'un quelconque de ces nombres, on aura, pour certaines valeurs de n,

$$a^n \equiv \mathrm{N} \pmod{\mathrm{M}}.$$

Chacun des nombres n ainsi déterminés prend le nom d'*indice* du nombre N, et la racine primitive a est dite la *base* des indices.

Un nombre a une infinité d'indices, mais tous ces indices sont congrus suivant le module $\varphi(\mathrm{M})$; on peut donc se borner à considérer l'*indice minimum* qui est l'un des nombres

$$0,\ 1,\ 2,\ \ldots,\ \varphi(\mathrm{M})-1.$$

Il est évident que l'indice minimum de l'unité est zéro.

Si l'on a calculé les indices des nombres N premiers à M, au moyen de la base a, et que l'on veuille prendre pour base une autre racine primitive a', on pourra obtenir facilement les indices qui se rapportent à cette base. Car soit e l'indice de la nouvelle base a', dans le premier système ; on aura

$$a' \equiv a^e \pmod{\mathrm{M}},$$

et si n et n' sont les indices d'un même nombre relatifs aux bases respectives a et a', on aura

$$a'^{n'} \equiv a^n \pmod{\text{M}},$$

ou

$$a^{n'e} \equiv a^n \pmod{\text{M}};$$

ce qui exige que l'on ait

$$n'e \equiv n \quad \text{ou} \quad n' \equiv \frac{n}{e} \quad [\text{mod. } \varphi(\text{M})],$$

puisque e est premier avec $\varphi(\text{M})$.

Par conséquent, les nouveaux indices s'obtiendront en divisant les anciens par l'indice de la nouvelle base relatif au premier système.

327. Les propriétés des indices sont analogues à celles des logarithmes; elles découlent toutes de la proposition suivante :

Théorème. — *L'indice d'un produit de plusieurs facteurs, pris suivant le module* M, *est congru, suivant le module* $\varphi(\text{M})$, *à la somme des indices des facteurs.*

En effet, soient α, β, γ, ... les indices des nombres A, B, C, ..., dans le système dont la base est a. On aura

$$a^\alpha \equiv \text{A}, \quad a^\beta \equiv \text{B}, \quad a^\gamma \equiv \text{C}, \quad \ldots \pmod{\text{M}},$$

et, en multipliant toutes ces congruences, il vient

$$a^{\alpha+\beta+\gamma+\ldots} \equiv \text{ABC}\ldots \pmod{\text{M}},$$

ce qui montre que l'indice minimum du produit ABC... est le résidu de $\alpha + \beta + \gamma + \ldots$ relativement à $\varphi(\text{M})$. On a donc

$$\text{ind.}(\text{ABC}\ldots) \equiv \text{ind. A} + \text{ind. B} + \text{ind. C} + \ldots \quad [\text{mod. } \varphi(\text{M})].$$

Corollaire I. — *L'indice d'une puissance d'un nombre, suivant le module* M, *est congru, suivant le module*

$\varphi(M)$, *au produit du nombre par l'exposant de la puissance.*

Corollaire II. — *L'indice du quotient de deux nombres, suivant le module* M, *est congru, suivant le module* $\varphi(M)$, *à l'excès de l'indice du premier nombre sur l'indice du second.*

En effet, l'égalité

$$\frac{A}{B} \times B = A$$

entraîne

$$\text{ind.}\, \frac{A}{B} + \text{ind.}\, B \equiv \text{ind.}\, A \quad [\text{mod.}\, \varphi(M)],$$

ou

$$\text{ind.}\, \frac{A}{B} \equiv \text{ind.}\, A - \text{ind.}\, B \quad [\text{mod.}\, \varphi(M)].$$

On voit, d'après cela, que si l'on a deux Tables dont l'une donne les indices des nombres pour chaque module, et dont l'autre fasse connaître les nombres qui répondent à des indices donnés, on pourra résoudre facilement les congruences du premier degré, puisqu'on peut les ramener à d'autres dont les modules soient des nombres premiers ou des puissances de nombres premiers.

Usage des indices dans la résolution des congruences binômes.

328. Les racines de la congruence binôme

$$(1) \qquad x^t \equiv A \quad (\text{mod.}\, M)$$

peuvent, si l'on veut, être représentées par la formule

$$(2) \qquad x \equiv \sqrt[t]{A} \quad (\text{mod.}\, M);$$

le module M est, comme précédemment, une puissance

d'un nombre premier impair ou le double d'une telle puissance. Il s'agit de déterminer les nombres compris ainsi dans le symbole $\sqrt[t]{A}$ (mod. M).

La congruence (1) équivaut, d'après ce qui précède, à la suivante :

$$(3) \qquad t.\,\text{ind.}\,x \equiv \text{ind.}\,A \quad [\text{mod.}\ \varphi(M)];$$

on est donc ramené, si l'on possède une Table des indices, à la résolution d'une congruence du premier degré.

Lorsque t est premier avec $\varphi(M)$, la congruence (3) donne pour ind. x une valeur unique, et par suite la proposée (1) n'a qu'une seule racine. Mais, lorsque t et $\varphi(M)$ ont un plus grand commun diviseur δ supérieur à 1, la congruence (3) n'est possible que si ind. A est divisible par δ, et, dans ce cas, la congruence (1) a δ racines.

Supposons, par exemple, $A = 1$; la proposée devient

$$x^t \equiv 1 \quad (\text{mod.}\ p^\nu \text{ ou } 2p^\nu),$$

et l'on en tire

$$t.\,\text{ind.}\,x \equiv 0 \quad [\text{mod.}\ p^{\nu-1}(p-1)].$$

Si donc δ est le plus grand commun diviseur des nombres t et $p^{\nu-1}(p-1)$, on aura ces valeurs de ind. x :

$$\text{ind.}\,x = \frac{(p-1)p^{\nu-1}}{\delta}, \quad 2\frac{(p-1)p^{\nu-1}}{\delta}, \quad \ldots, \quad \delta\frac{(p-1)p^{\nu-1}}{\delta},$$

desquelles on conclura ensuite les δ valeurs de x.

Démonstration d'un théorème de Lagrange.

329. Nous ne pourrions, sans sortir des limites que nous nous sommes fixées, développer ici toutes les conséquences de la théorie qui vient d'être exposée. Mais

nous en ferons cependant deux applications dont la première a pour objet la démonstration d'un théorème important de Lagrange. Cette démonstration est fondée sur le lemme suivant :

Lemme. — *Si le nombre premier p est supérieur à 5, on trouve dans la suite*

$$1,\ 2,\ 3,\ \ldots,\ (p-1):$$

1° *un résidu* R *suivi d'un résidu;* 2° *un résidu* R' *suivi d'un non-résidu;* 3° *un non-résidu* N *suivi d'un non-résidu;* 4° *un non-résidu* N' *suivi d'un résidu.*

En effet, soient β un *non-résidu* ou de la forme $1, 2, \ldots, (p-2)$, et γ l'associé de β, c'est-à-dire un non-résidu. Je dis que les *successions*

$$(\beta,\ \beta+1) \quad \text{et} \quad (\gamma,\ \gamma+1),$$

qui ont leur premier terme β et γ non-résidu, sont *conjuguées*. En effet, à cause de

$$\beta\gamma \equiv 1 \pmod{p},$$

si $\beta+1$ est non-résidu, $\gamma+1 \equiv \gamma+\beta\gamma \equiv (\beta+1)\gamma$, (mod. p), $\gamma+1$ sera le produit de deux non-résidus : il est donc résidu. Si $\beta+1$ est résidu, la précédente congruence exprime que $\gamma+1$ est non-résidu. On a donc

$$\text{(1)} \qquad \text{N}' = \text{N}.$$

Il y a lieu de distinguer le cas de $p = 4q+1$, et celui de $p = 4q+3$.

Supposons $p = 4q+1$ et désignons par $a, a', \ldots$ les résidus et par $b, b', \ldots$ les non-résidus. Dans le cas que nous examinons et dont la somme égale p, deux nombres sont résidus ou non-résidus; on peut donc poser

$$p = a + a' = b + b'.$$

Cela étant, chacune des *successions* entraîne l'autre

$$(a, b) \quad \text{et} \quad (b', a').$$

Si l'on fait $b = a + 1$, la précédente égalité se réduit à $a' = b' + 1$; donc

$$(2) \qquad R' = N'.$$

En second lieu, comme il y a $\frac{p-1}{2}$ résidus et autant de non-résidus et que le dernier terme $p-1$ de la suite est résidu, on a

$$(3) \qquad \begin{cases} N + N' = \dfrac{p-1}{2}, \\ R + R' = \dfrac{p-1}{2} - 1. \end{cases}$$

Ces dernières équations, jointes aux équations (1) et (2), donnent ainsi

$$(4) \qquad \begin{cases} N = N' = R' = \dfrac{p-1}{4}, \\ R = \dfrac{p-1}{4} - 1. \end{cases}$$

Supposons $p = 4q + 3$. Alors deux nombres complémentaires à p sont l'un résidu, l'autre non-résidu. On peut donc poser

$$p = a + b = a' + b';$$

alors chacune des *successions*

$$(b, b') \quad \text{et} \quad (a', a)$$

entraîne l'autre et l'on a, par conséquent,

$$(5) \qquad R = N.$$

Ensuite le dernier terme de la suite étant non-résidu,

on a

$$(6)\quad \begin{cases} R + R' = \dfrac{p-1}{2} = \dfrac{p-3}{2} + 1, \\ N + N' = \dfrac{p-1}{2} - 1 = \dfrac{p-3}{2}. \end{cases}$$

Ces dernières équations donnent avec (1) et (5)

$$(7)\quad \begin{cases} N = N' = R = \dfrac{p-3}{4}, \\ R' = \dfrac{p-3}{4} + 1. \end{cases}$$

Remarque. — Ce lemme subsiste dans le cas de $p = 3$: on a $N = N' = R = 0$ et $R' = 1$; il a lieu encore si $p = 5$: on a $N = N' = R' = 1$ et $R = 0$.

Corollaire. — *Si* C *désigne un nombre quelconque non divisible par p, la proposition précédente subsiste quand, à la suite*

(1) $1, 2, 3, \ldots, (p-1)$,

on substitue la suivante :

(2) $C, 2C, 3C, \ldots (p-1)C$.

En effet, si C est résidu, deux termes correspondants des suites (1) et (2) sont à la fois résidus ou non-résidus. Au contraire, si C est non-résidu, les résidus de la suite (2) correspondent aux non-résidus de la suite (1), et inversement.

330. Théorème. — *Si p est un nombre premier supérieur à* 5, A, B, C *trois entiers positifs ou négatifs non divisibles par p, on peut toujours trouver deux entiers t et u inférieurs à* $\frac{p}{2}$, *tels que*

$$At^2 + Bu^2 + C$$

soit divisible par p.

1° Si B et — C sont tous deux résidus, ou tous deux non-résidus quadratiques par rapport à p, on peut prendre $t = 0$; en effet, il ne restera plus alors qu'à satisfaire à la congruence

$$Bu^2 + C \equiv 0 \pmod{p}, \quad \text{ou} \quad Bu^2 + (C + \lambda p) \equiv 0 \pmod{p},$$

λ étant un entier quelconque. Si l'on détermine cet entier de manière que l'on ait

$$-\frac{C + \lambda p}{B} = \mu,$$

μ étant un entier, notre congruence deviendra

$$u^2 \equiv \mu \pmod{p},$$

et il sera possible d'y satisfaire, car, B et — C étant l'un et l'autre résidus ou non résidus, μ est nécessairement résidu.

Pareillement, si A et — C sont tous deux résidus ou tous deux non-résidus, on pourra satisfaire à la condition énoncée, en prenant $u = 0$, quel que soit le nombre premier p.

2° Si p est > 5, on peut toujours satisfaire à la congruence

$$At^2 + Bu^2 + C \equiv 0 \pmod{p},$$

en prenant pour t et u des valeurs positives inférieures à $\frac{p}{2}$. En effet, soient α et 6 deux nombres qui soient respectivement de même espèce que $+A$ et $-B$; je dis que deux nombres sont de même espèce quand ils sont l'un et l'autre résidus ou non-résidus. D'après le lemme qui précède, je puis choisir les nombres α et 6 de manière que l'on ait

$$6 - \alpha \equiv C \pmod{p},$$

et si l'on désigne par λ et μ des nombres entiers tels que

$$\frac{\alpha + p\lambda}{A}, \quad \frac{\beta + p\mu}{-B}$$

soient des entiers, ces entiers seront nécessairement résidus; on aura donc

$$\frac{\alpha + p\lambda}{A} \equiv t^2, \quad \frac{\beta + p\mu}{-B} \equiv u^2 \pmod{p},$$

ou

$$\alpha \equiv At^2, \quad \beta \equiv -Bu^2 \pmod{p};$$

et comme $\beta - \alpha \equiv C$, on aura aussi

$$At^2 + Bu^2 + C \equiv 0 \pmod{p},$$

ce qu'il fallait démontrer.

Remarque. — D'après ce théorème, la formule $t^2 + u^2 + 1$ comprend des nombres divisibles par p, quand p est > 5. Mais la même chose a lieu encore dans le cas de $p = 5$, pour $t = 0$, $u = 2$; dans le cas de $p = 3$, pour $t = u = 1$, et dans le cas de $p = 2$, pour $t = 0$, $u = 1$. D'ailleurs la formule $t^2 + u^2 + 1$ est comprise dans cette autre plus générale, $P^2 + Q^2 + R^2 + S^2$; d'où il résulte que *tout nombre premier divise une somme de quatre carrés premiers entre eux.*

331. Cette conclusion va nous conduire à une conséquence importante qui se présentera comme corollaire de la proposition suivante :

Théorème. — *Tout nombre qui divise la somme de quatre carrés premiers entre eux est lui-même la somme de quatre carrés.*

Supposons que p divise

$$A^2 + B^2 + C^2 + D^2,$$

et désignons par $\pm a$, $\pm b$, $\pm c$, $\pm d$ les résidus minima des nombres A, B, C, D, de manière que a, b, c, d soient compris entre zéro et $\frac{p}{2}$; alors p divisera

$$a^2 + b^2 + c^2 + d^2.$$

Posons

$$(1) \qquad a^2 + b^2 + c^2 + d^2 = pp';$$

a, b, c, d étant moindres que $\frac{p}{2}$, on aura $pp' < 4\left(\frac{p}{2}\right)^2$, ou

$$p' < p.$$

Si l'on avait $p' = 1$, p serait la somme de quatre carrés, et le théorème serait démontré; supposons donc $p' > 1$. Comme p' divise $a^2 + b^2 + c^2 + d^2$, il divisera aussi la somme des quatre carrés

$$(a - \alpha p')^2 + (b - \beta p')^2 + (c - \gamma p')^2 + (d - \delta p')^2,$$

et si l'on détermine α, β, γ, δ de manière que chacun de ces carrés soit moindre que $\frac{p'^2}{4}$, on pourra écrire

$$(2) \quad (a - \alpha p')^2 + (b - \beta p')^2 + (c - \gamma p')^2 + (d - \delta p')^2 = p'p'',$$

avec

$$p'' < p'.$$

Multipliant ensemble les équations (1) et (2), et faisant usage de la formule établie au n° 215, il vient

$$\begin{aligned}(a\delta - b\gamma + c\beta - d\alpha)^2 p'^2 &+ (a\gamma + b\delta - c\alpha - d\beta)^2 p'^2 \\ &+ (a\beta - b\alpha - c\delta + d\gamma)^2 p'^2 \\ &+ [a^2 + b^2 + c^2 + d^2 - (a\alpha + b\beta + c\gamma + d\delta)p']^2 = pp'^2 p'';\end{aligned}$$

divisant par p'^2, et ayant égard à l'équation (1), on a

$$\begin{aligned}(a\delta - b\gamma + c\beta - d\alpha)^2 &+ (a\gamma + b\delta - c\alpha - d\beta)^2 \\ &+ (a\beta - b\alpha - c\delta + d\gamma)^2 + (p - a\alpha - b\beta - c\gamma - d\delta)^2 = pp'',\end{aligned}$$

ou, pour abréger,

(3) $$a'^2 + b'^2 + c'^2 + d'^2 = pp''.$$

Cette équation (3) a la même forme que (1), seulement p'' est $< p'$. Si l'on a $p'' = 1$, l'équation (3) montre que p est la somme de quatre carrés, et le théorème est démontré. Sinon, en opérant sur l'équation (3) comme nous avons fait sur l'équation (1), on obtiendra une nouvelle équation de la forme

$$a''^2 + b''^2 + c''^2 + d''^2 = pp''',$$

où l'on aura

$$p''' < p'';$$

et l'on peut continuer de cette manière jusqu'à ce qu'on obtienne une équation de la forme

$$a^{(n)2} + b^{(n)2} + c^{(n)2} + d^{(n)2} = p,$$

ce qui arrivera nécessairement, puisque les nombres

$$p',\ p'',\ p''',\ \ldots$$

sont des entiers qui vont en décroissant; d'où il suit enfin que le nombre p est la somme de quatre carrés.

Corollaire. — *Tout nombre entier est la somme de quatre ou d'un moindre nombre de carrés.*

En effet, tout nombre premier (n° 330) divise la somme de quatre carrés premiers entre eux; il est donc lui-même la somme de quatre ou d'un moindre nombre de carrés.

En second lieu, un nombre entier quelconque est le produit de plusieurs facteurs premiers; chacun de ces facteurs est la somme de quatre carrés; donc leur produit (n° 245) est lui-même la somme de quatre carrés.

Théorème de Legendre sur la loi de réciprocité qui existe entre deux nombres premiers.

332. La loi de réciprocité découverte par Legendre consiste dans le théorème suivant :

THÉORÈME. — *Si p et q sont deux nombres premiers impairs quelconques, on a*

$$\left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{q}{p}\right),$$

en sorte que

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right),$$

à moins que p et q ne soient tous deux de la forme $4k+3$; on a dans ce dernier cas

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

La démonstration que nous allons présenter est due à Gauss, et elle a été reproduite par Legendre dans le tome II de sa *Théorie des nombres*. Nous établirons d'abord le lemme suivant :

Soient p un nombre premier positif autre que 2, et q un entier quelconque non divisible par p ; les produits

$$(1) \qquad q,\ 2q,\ 3q,\ \ldots,\ \frac{p-1}{2}q$$

donneront, suivant le module p, $\frac{p-1}{2}$ restes différents compris entre les limites $-\frac{p-1}{2}$ et $+\frac{p-1}{2}$, et si l'on désigne par μ le nombre de ceux de ces restes qui sont négatifs, on aura

$$\left(\frac{q}{p}\right) = (-1)^{\mu}.$$

En effet, soient

$$(2) \qquad a_1,\ a_2,\ \ldots,\ a_\lambda$$

les $\lambda = \frac{p-1}{2} - \mu$ restes positifs, et

$$(3) \qquad -b_1,\ -b_2\ \ldots,\ -b_\mu$$

les μ restes négatifs.

Il est évident que l'un des restes ne peut être zéro; de plus, deux résidus pris dans l'une des suites (2) ou (3) ne peuvent être égaux entre eux; mais je dis, en outre, qu'on ne peut avoir $a_m = b_n$. Effectivement, soient αq, $6q$ les multiples de q qui ont fourni les restes a_m et $-b_n$; l'égalité $a_m = b_n$ entraînerait

$$\alpha q \equiv -6q \quad \text{ou} \quad (\alpha + 6)q \equiv 0 \quad (\text{mod.}\, p),$$

ce qui est impossible, puisque q n'est pas divisible par p et que la somme $\alpha + 6$ est inférieure à p. Il résulte de là que la suite formée des nombres a et b comprend les mêmes nombres que la suite

$$1,\ 2,\ 3,\ \ldots,\ \frac{p-1}{2}.$$

Les nombres de la suite (1) étant respectivement congrus aux nombres compris dans les suites (2) et (3), le produit des uns est congru au produit des autres, et l'on a

$$\left(1.2.3\ldots\frac{p-1}{2}\right) q^{\frac{p-1}{2}} \equiv (-1)^\mu a_1 a_2 \ldots a_\lambda b_1 b_2 \ldots b_\mu \ (\text{mod.}\ p),$$

et en divisant les deux membres respectivement par les produits

$$1.2.3\ldots\frac{p-1}{2}, \quad a_1 a_2 \ldots a_\lambda b_1 b_2 \ldots b_\mu,$$

qui sont égaux entre eux, comme on vient de le dire, on

aura

$$q^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p},$$

ou

(4) $$\left(\frac{q}{p}\right) = (-1)^{\mu},$$

ce qui est le résultat annoncé.

Maintenant il est aisé de trouver une expression analytique du nombre μ. Dans ce qui va suivre, nous désignerons par $E(x)$ le plus grand entier contenu dans une quantité quelconque x, de manière que la différence $x - E(x)$ soit une quantité positive inférieure à 1. Cela posé, soient αq et βq les produits qui fournissent les restes a et $-b$, on aura

$$\frac{\alpha q}{p} = E\left(\frac{\alpha q}{p}\right) + \frac{a}{p}, \quad \frac{\beta q}{p} = E\left(\frac{\beta q}{p}\right) + \frac{p-b}{p},$$

ou, en multipliant par 2,

$$\frac{2\alpha q}{p} = 2E\left(\frac{\alpha q}{p}\right) + \frac{2a}{p}, \quad \frac{2\beta q}{p} = 2E\left(\frac{\beta q}{p}\right) + 1 + \frac{p-2b}{p}.$$

Comme $2a$ et $2b$ sont inférieurs à p, on voit que

$$2E\left(\frac{\alpha q}{p}\right) \quad \text{et} \quad 2E\left(\frac{\beta q}{p}\right) + 1$$

sont respectivement les plus grands entiers contenus dans $\frac{2\alpha q}{p}$ et $\frac{2\beta q}{p}$; on a donc

$$\left(\frac{2\alpha q}{p}\right) - 2E\left(\frac{\alpha q}{p}\right) = 0,$$
$$E\left(\frac{2\beta q}{p}\right) - 2E\left(\frac{\beta q}{p}\right) = 1.$$

Donnons à α et à β toutes les valeurs dont ces nombres sont susceptibles; les formules précédentes fourniront

$\lambda + \mu$ équations distinctes, et, en ajoutant toutes ces équations, il viendra

$$\mu = \mathrm{E}\left(\frac{2q}{p}\right) + \mathrm{E}\left(\frac{4q}{p}\right) + \ldots + \mathrm{E}\left[\frac{(p-3)q}{p}\right] + \mathrm{E}\left[\frac{(p-1)q}{p}\right]$$
$$- 2\mathrm{E}\left(\frac{q}{p}\right) - 2\mathrm{E}\left(\frac{2q}{p}\right) - \ldots - 2\mathrm{E}\left(\frac{p-1}{2}\frac{q}{p}\right).$$

Mais, comme on n'a besoin de la valeur de μ que pour savoir si elle est paire ou impaire, on peut, dans cette formule, supprimer tous les termes de la seconde ligne, lesquels sont des nombres pairs, et nous écrirons simplement

$$(5)\quad \left\{\begin{aligned} \mu \equiv \mathrm{E}\left(\frac{2q}{p}\right) + \mathrm{E}\left(\frac{4q}{p}\right) + \ldots \\ + \mathrm{E}\left[\frac{(p-3)q}{p}\right] + \mathrm{E}\left[\frac{(p-1)q}{p}\right] \end{aligned}\right\} \pmod{2}.$$

Si l'on pose

$$\frac{nq}{p} = \mathrm{E}\left(\frac{nq}{p}\right) + \theta,$$

on aura, en retranchant de q chaque membre de cette formule,

$$\frac{(p-n)q}{p} = (q-1) - \mathrm{E}\left(\frac{nq}{p}\right) + (1-\theta),$$

d'où il résulte que l'on a, quel que soit n,

$$\mathrm{E}\left[\frac{(p-n)q}{p}\right] = (q-1) - \mathrm{E}\left(\frac{nq}{p}\right);$$

en ajoutant au second membre le nombre pair $2\mathrm{E}\left(\frac{nq}{p}\right)$, on obtient cette congruence

$$(6)\quad \mathrm{E}\left[\frac{(p-n)q}{p}\right] \equiv (q-1) + \mathrm{E}\left(\frac{nq}{p}\right) \pmod{2}.$$

Posons $p = 4i \pm 1$, et donnons à n les valeurs 1, 3, 5, .. , $(2i-1)$, la congruence (5) deviendra, en faisant usage des résultats ainsi obtenus,

$$(7)\quad \left\{\begin{aligned}\mu \equiv (q-1) + \mathrm{E}\left(\frac{q}{p}\right) + \mathrm{E}\left(\frac{2q}{p}\right) + \mathrm{E}\left(\frac{3q}{p}\right) + \ldots \\ + \mathrm{E}\left(\frac{p-1}{2}\frac{q}{p}\right)\end{aligned}\right\} \pmod{2}.$$

Cette formule (7) a lieu, quel que soit le nombre q, pourvu qu'il ne soit pas divisible par p, et cette remarque nous sera utile plus loin; si q est impair, $q-1$ est un nombre pair et la formule (7) se réduit à

$$(8)\quad \left\{\begin{aligned}\mu \equiv \mathrm{E}\left(\frac{q}{p}\right) + \mathrm{E}\left(\frac{2q}{p}\right) + \mathrm{E}\left(\frac{3q}{p}\right) + \ldots \\ + \mathrm{E}\left(\frac{p-1}{2}\frac{q}{p}\right)\end{aligned}\right\} \pmod{2};$$

cette valeur de μ peut être mise, comme on va le voir, sous une autre forme. Nous supposerons, dans ce qui va suivre, $q < p$; alors le premier terme du second membre de la formule (8) est zéro, et le dernier terme est $\frac{q-1}{2}$, car on a

$$\frac{p-1}{2}\frac{q}{p} = \frac{q-1}{2} + \frac{p-q}{2p}.$$

Cela posé, soit n un entier donné égal ou inférieur à $\frac{q-1}{2}$, et désignons par m le nombre des termes de la précédente valeur de μ qui sont inférieurs à n. Le nombre $m+1$ étant inférieur à p, l'expression $\frac{(m+1)q}{p}$ ne pourra jamais se réduire à un entier, et l'on aura, en conséquence,

$$\mathrm{E}\left(\frac{mq}{p}\right) < n,\quad \mathrm{E}\left[\frac{(m+1)q}{p}\right] > n,$$

d'où

$$\frac{mq}{p} < n, \quad \frac{(m+1)q}{p} > n,$$

ou

$$m < \frac{np}{q} < m+1;$$

ces inégalités expriment que m est le plus grand entier contenu dans $\frac{np}{q}$; on a donc

$$m = \mathrm{E}\left(\frac{np}{q}\right).$$

Pareillement le second membre de la formule (8) contiendra $\mathrm{E}\left[\frac{(n+1)p}{q}\right]$ termes inférieurs à $n+1$, si $n+1$ n'est pas supérieur à $\frac{q-1}{2}$, c'est-à-dire si l'on a

$$n < \frac{q-1}{2}.$$

Dans cette hypothèse, notre expression de μ contiendra d'après cela

$$(9) \qquad \mathrm{E}\left[\frac{(n+1)p}{q}\right] - \mathrm{E}\left(\frac{np}{q}\right)$$

termes égaux à n. En outre, le nombre total des termes de l'expression de μ est $\frac{p-1}{2}$, et, comme le nombre de ceux qui sont inférieurs à $\frac{q-1}{2}$ est $\mathrm{E}\left(\frac{q-1}{2}\frac{p}{q}\right)$, il y aura, dans μ,

$$(10) \qquad \frac{p-1}{2} - \mathrm{E}\left(\frac{q-1}{2}\frac{p}{q}\right)$$

termes égaux à $\frac{q-1}{2}$.

Si l'on multiplie l'expression (9) par n, qu'on rem-

place ensuite n par chacune des valeurs

$$1,\ 2,\ 3,\ \ldots,\ \left(\frac{p-1}{2}-1\right),$$

qu'on ajoute enfin tous les résultats avec le produit de l'expression (10) par $\frac{q-1}{2}$, il est évident qu'on reproduira la valeur de μ. On a donc

$$\left.\begin{array}{l}\mu \equiv \left[\mathrm{E}\left(\frac{2p}{q}\right) - \mathrm{E}\left(\frac{p}{q}\right)\right] \\ \quad + 2\left[\mathrm{E}\left(\frac{3p}{q}\right) - \mathrm{E}\left(\frac{2p}{q}\right)\right] \\ \quad \cdots\cdots\cdots\cdots\cdots\cdots \\ \quad + \frac{q-3}{2}\left[\mathrm{E}\left(\frac{q-1}{2}\frac{p}{q}\right) - \mathrm{E}\left(\frac{q-3}{2}\frac{p}{q}\right)\right] \\ \quad + \frac{q-1}{2}\left[\frac{p-1}{2} - \mathrm{E}\left(\frac{q-1}{2}\frac{p}{q}\right)\right]\end{array}\right\} \pmod{2},$$

ou, en réduisant

$$(11)\quad \mu \equiv \frac{p-1}{2}\frac{q-1}{2} - \left[\mathrm{E}\left(\frac{p}{q}\right) + \mathrm{E}\left(\frac{2p}{q}\right) + \ldots + \mathrm{E}\left(\frac{q-1}{2}\frac{p}{q}\right)\right] \pmod{2}.$$

La formule (8) s'applique à un nombre premier impair p et à un nombre impair quelconque q; si donc on suppose q premier et que l'on fasse

$$(12)\qquad \left(\frac{p}{q}\right) = (-1)^{\nu},$$

le nombre ν sera donné par la formule (8) en permutant, dans celle-ci, les lettres p et q; on aura ainsi

$$(13)\qquad \nu \equiv \mathrm{E}\left(\frac{p}{q}\right) + \mathrm{E}\left(\frac{2p}{q}\right) + \ldots + \mathrm{E}\left(\frac{q-1}{2}\frac{p}{q}\right) \pmod{2}.$$

La comparaison des formules (11) et (13) donne

$$\mu + \nu \equiv \frac{p-1}{2}\,\frac{q-1}{2} \pmod{2};$$

d'ailleurs on a, par les formules (4) et (12),

$$\left(\frac{q}{p}\right) = (-1)^{\mu+\nu}\left(\frac{p}{q}\right):$$

donc

(14) $$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

ce qui est la formule que nous voulions établir.

Remarque. — Il faut remarquer que le nombre -1 est résidu de tous les nombres premiers $4i+1$, et qu'il est non-résidu des nombres premiers $4i+3$.

On a effectivement, par la définition du n° 311,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}};$$

cette égalité est d'ailleurs comprise dans notre formule (8); car, si $q=-1$, chacun des termes du second membre de cette formule se réduit à -1, et l'on a

$$\mu \equiv -\frac{p-1}{2} \equiv \frac{p-1}{2} \pmod{2}.$$

On conclut de là que la congruence

$$x^2+1 \equiv 0 \pmod{p}$$

est possible ou impossible suivant que p a la forme $4i+1$ ou la forme $4i+3$. Si le premier cas a lieu, le nombre p divise la somme de deux carrés, et il est, par suite, la somme de deux carrés, résultat auquel nous a déjà conduit le théorème de Wilson.

333. La formule (7) du numéro précédent exige seulement, comme nous l'avons déjà dit, que q ne soit pas divisible par p. Si l'on y suppose $q = 2$, les expressions $E\left(\frac{q}{p}\right), \ldots$ qui y figurent se réduiront toutes à zéro; on aura donc

$$\mu \equiv i \equiv \frac{p \mp 1}{4} \quad (\text{mod. } 2);$$

d'ailleurs, $\frac{p \pm 1}{2}$ est un nombre impair, et l'on peut écrire

$$\mu \equiv \frac{(p+1)(p-1)}{8} \quad (\text{mod. } 2).$$

Si, en second lieu, on pose $q = -2$, les expressions $E\left(\frac{q}{p}\right), E\left(\frac{2q}{p}\right), \ldots$ de la formule (7) se réduiront toutes à -1, et l'on aura

$$\mu \equiv i - \frac{p-1}{2} \equiv \frac{(p+1)(p-1)}{8} - \frac{p-1}{2} \quad (\text{mod. } 2),$$

ou

$$\mu \equiv \frac{(p-1)(p-3)}{8} \quad (\text{mod. } 2).$$

D'après cela on a, pour tout nombre premier impair p,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p+1)(p-1)}{8}}, \quad \left(\frac{-2}{p}\right) = (-1)^{\frac{(p-1)(p-3)}{8}},$$

formules qui expriment le théorème suivant :

THÉORÈME. — *Le nombre* $+2$ *est résidu quadratique de tout nombre premier de l'une des formes* $8k+1$, $8k+7$; *il est non-résidu de tout nombre premier de l'une des formes* $8k+3$, $8k+5$.

Le nombre -2 *est résidu quadratique de tout nombre premier de l'une des formes* $8k+1$, $8k+3$;

il est non-résidu de tout nombre premier de l'une des formes $8k+5$, $8k+7$.

334. Il ne sera pas inutile de présenter ici quelques-unes des applications du théorème de Legendre.

On a, relativement aux nombres premiers 3 et $p=3n\pm 1$,

$$\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{\pm 1}{3}\right);$$

d'ailleurs, relativement au module 3, $+1$ est résidu et -1 non-résidu; si donc on distingue les nombres premiers en quatre classes, savoir :

$$12k+1,\quad 12k+5,\quad 12k+7,\quad 12k+11,$$

on aura cette proposition :

Le nombre $+3$ *est résidu quadratique de tous les nombres premiers* $12k+1$, *et* $12k+11$, *et il est non-résidu de tous les nombres premiers* $12k+5$, $12k+7$.

Et, d'après ce qui a été dit au n° 311, on peut ajouter :

Le nombre -3 *est résidu quadratique de tous les nombres premiers* $12k+1$, $12k+7$, *et il est non-résidu de tous les nombres premiers* $12k+5$, $12k+11$.

Ces deux propositions ont été démontrées pour la première fois, par Euler, dans le tome VIII des *Nouveaux Commentaires de Saint-Pétersbourg.*

Relativement aux nombres premiers 5 et p, on a

$$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right),$$

mais on a

$$\left(\frac{p}{5}\right)=\pm 1,$$

suivant que p est de la forme $5n\pm 1$ ou de la forme

$5n \pm 2$; si donc on distingue les nombres premiers dans les huit classes

$$20k-1,\quad 20k+3,\quad 20k+7,\quad 20k+9,$$
$$20k+11,\quad 20k+13,\quad 20k+17,\quad 20k+19,$$

suivant le reste que donne leur division par 20, on aura cette proposition :

Le nombre $+5$ *est résidu quadratique de tous les nombres premiers de l'une des formes* $20k+1$, $20k+9$, $20k+11$, $20k+19$, *et il est non-résidu de tous les nombres premiers de l'une des formes* $20k+3$, $20k+7$, $20k+13$, $20k+17$.

Et, conséquemment :

Le nombre -5 *est résidu quadratique de tous les nombres premiers de l'une des formes* $20k+1$, $20k+3$, $20k+7$, $20k+9$, *et il est non-résidu des nombres premiers de l'une des formes* $20k+11$, $20k+13$, $20k+17$, $20k+19$.

De la congruence $x^2 - N \equiv 0$ (mod. p), *p étant un nombre premier.*

335. Le théorème de Legendre fournit le moyen de reconnaître, par un calcul facile, si la congruence

$$x^2 - N \equiv 0 \pmod{p}$$

est soluble ou non ; car la condition de résolubilité est exprimée par l'égalité

$$\left(\frac{N}{p}\right) = +1.$$

Tout revient donc à déterminer le signe du symbole $\left(\frac{N}{p}\right)$. Le nombre N peut toujours être rabaissé au-dessous de p;

en outre, si l'on a

$$N = a^\alpha b^\beta c^\gamma, \ldots,$$

$a, b, c, \ldots$ étant des facteurs premiers inégaux, on aura

$$\left(\frac{N}{p}\right) = \left(\frac{a^\alpha}{p}\right)\left(\frac{b^\beta}{p}\right)\left(\frac{c^\gamma}{p}\right)\cdots;$$

mais on a évidemment

$$\left(\frac{a^\alpha}{p}\right) = +1$$

si α est pair, et

$$\left(\frac{a^\alpha}{p}\right) = \left(\frac{a}{p}\right)$$

si α est impair; la détermination de $\left(\frac{N}{p}\right)$ est donc ramenée à celle des symboles plus simples

$$\left(\frac{a}{p}\right), \quad \left(\frac{b}{p}\right), \quad \ldots,$$

a et b étant ceux des facteurs premiers de N qui figurent dans ce nombre avec des exposants impairs.

Considérons l'un de ces symboles, $\left(\frac{a}{p}\right)$ par exemple. Sa valeur sera immédiatement connue (n° 333), si $a = 2$. Dans le cas contraire, la recherche de $\left(\frac{a}{p}\right)$ est ramenée, par le théorème de Legendre, à celle de $\left(\frac{p}{a}\right)$. On opérera alors, à l'égard de $\left(\frac{p}{a}\right)$, comme nous venons de le faire relativement à $\left(\frac{N}{p}\right)$, et, en continuant ainsi, on tombera nécessairement sur des symboles dont la valeur sera connue.

Exemple. — Soit la congruence

$$x^2 + 1459 \equiv 0 \pmod{22366891},$$

qui est l'une de celles que Legendre a considérées dans sa *Théorie des nombres*.

Le module est ici un nombre premier $4k+3$, et 1459 est lui-même un nombre premier de cette forme; on a donc

$$\left(\frac{N}{p}\right) = \left(\frac{-1459}{22366891}\right) = -\left(\frac{1459}{22366891}\right) = \left(\frac{22366891}{1459}\right).$$

Le reste de la division de 22366891 par 1459 est 421; donc

$$\left(\frac{N}{p}\right) = \left(\frac{421}{1459}\right);$$

421 est un nombre premier $4k+1$; par conséquent,

$$\left(\frac{N}{p}\right) = \left(\frac{1459}{421}\right) = \left(\frac{196}{421}\right) = \left(\frac{4 \times 49}{421}\right) = 1,$$

puisque 4×49 est un carre.

La congruence proposée admet donc deux racines.

336. La congruence

$$x^2 - N \equiv 0 \pmod{p}$$

ayant été reconnue possible, supposons qu'on veuille la résoudre. Nous distinguerons deux cas suivant que le module p est de la forme $4k+3$ ou de la forme $4k+1$.

Supposons d'abord

$$p = 4k + 3,$$

la congruence proposée étant possible, on a

$$N^{\frac{p-1}{2}} - 1 \equiv 0 \quad \text{ou} \quad N^{2k+1} - 1 \equiv 0 \pmod{p},$$

et, en multipliant par N,

$$N^{2k+2} - N \equiv 0 \pmod{p},$$

d'où il suit que les racines de notre congruence sont

$$x \equiv \pm N^{k+1}.$$

Soit actuellement le cas où p est de la forme $4k+1$; les nombres $4k+1$ comprennent les deux formes $8k+1$, $8k+5$, que nous allons considérer l'une après l'autre.

Supposons

$$p = 8k+5,$$

la congruence proposée étant possible, on a

$$N^{4k+2} - 1 \equiv 0 \pmod{p},$$

ou

$$(N^{2k+1}+1)(N^{2k+1}-1) \equiv 0 \pmod{p};$$

on a donc

$$N^{2k+1} - 1 \equiv 0 \pmod{p},$$

ou

$$N^{2k+1} + 1 \equiv 0 \pmod{p}.$$

Si c'est le premier cas qui a lieu, on aura

$$N^{2k+2} - N \equiv 0 \pmod{p},$$

et les racines de la proposée seront en conséquence

$$x \equiv \pm N^{k+1} \pmod{p}.$$

Si au contraire le deuxième cas se présente, posons

$$\theta \equiv N^{k+1} \pmod{p}, \quad \text{d'où} \quad \theta^2 \equiv N^{2k+2} \equiv -N \pmod{p},$$

la congruence proposée deviendra

$$x^2 + \theta^2 \equiv 0 \pmod{p}.$$

Or le nombre p, qui est de la forme $4k+1$, est la somme de deux carrés premiers entre eux. On peut donc poser

$$p = \alpha^2 + \beta^2,$$

d'où, t et u étant des indéterminées,

$$(\alpha^2+6^2)(t^2+u^2)=(\alpha t+6u)^2+(\alpha u-6t)^2\equiv 0 \pmod{p}.$$

On peut déterminer t et u par la condition

$$\alpha u - 6t = \theta,$$

et il est évident que la congruence proposée sera vérifiée en posant

$$x \equiv \pm(\alpha t+6u) \pmod{p}.$$

Il nous reste à examiner le cas où p a la forme $8k+1$. Alors il n'est pas possible, en général, de résoudre la congruence proposée sans tâtonnements, et l'on est obligé de calculer les termes de la suite

$$p+\text{N},\quad 2p+\text{N},\quad 3p+\text{N}\quad ,\ldots,$$

jusqu'à ce qu'on en trouve un qui soit un carré parfait. Cela ne peut manquer d'arriver lorsque la congruence proposée est possible, et, comme le carré que l'on cherche est moindre que $\frac{1}{4}p^2$, le nombre des termes à calculer, dans la suite précédente, ne pourra jamais excéder $\frac{1}{4}p$.

Il peut arriver cependant, dans le cas qui nous occupe, que l'on puisse trouver directement les racines demandées. Soit, en effet, 2^μ la plus haute puissance de 2 contenue dans $p-1$ et posons

$$p = 2^\mu\alpha + 1,$$

α étant un nombre impair et μ étant au moins égal à 3. La congruence proposée étant possible, on a

$$\text{N}^{2^{\mu-1}\alpha} \equiv 1 \pmod{p},$$

et il se peut que l'on ait aussi

$$\text{N}^\alpha \equiv \pm 1 \pmod{p}.$$

Admettant cette hypothèse, on aura

$$N^{\alpha+1} \equiv \pm N \pmod{p},$$

et, comme α est impair, on pourra procéder exactement comme nous l'avons fait dans le cas de $p = 8k + 5$.

Exemple. — Reprenons, avec Legendre, la congruence

$$x^2 + 1459 \equiv 0 \pmod{22366891}.$$

Nous avons vu que cette congruence a deux racines. Ici l'on a

$$p = 4k + 3$$

et

$$k + 1 = 5591723.$$

On trouve que

$$x = \pm 1459^{k+1} = \pm 7529774;$$

c'est ce que montre l'égalité

$$(7529774)^2 + 1459 = 22366891 \times 2534885.$$

De la congruence $x^2 - N \equiv 0$, dans le cas d'un module quelconque.

337. Supposons d'abord que le module soit une puissance p^ν d'un nombre premier impair p; la congruence proposée sera

(1) $$x^2 - N \equiv 0 \pmod{p^\nu}.$$

Commençons par résoudre cette congruence, suivant le module p, d'après la méthode du n° 336; si l'on désigne par $\pm \xi$ les racines, on aura

(2) $$\xi^2 - N \equiv 0 \pmod{p}$$

et, par suite,

$$(\xi^2 - N)^\nu \equiv 0 \pmod{p^\nu}.$$

Or, en développant la puissance $(\xi + \sqrt{N})^\nu$, on trouve un résultat de la forme

$$(3) \qquad (\xi + \sqrt{N})^\nu = \alpha + \beta\sqrt{N},$$

α et β étant des entiers, et il en résulte

$$(4) \qquad (\xi - \sqrt{N})^\nu = \alpha - \beta\sqrt{N},$$

par suite

$$(5) \qquad \alpha^2 - N\beta^2 = (\xi^2 - N)^\nu \equiv 0 \pmod{p^\nu}.$$

La formule (3) ou (4) donne aussi

$$\alpha = \xi^\nu + \frac{\nu(\nu-1)}{1.2}\xi^{\nu-2}N + \ldots,$$

$$\beta = \frac{\nu}{1}\xi^{\nu-1} + \frac{\nu(\nu-1)(\nu-2)}{1.2.3}\xi^{\nu-3}N + \ldots,$$

ou, à cause de la formule (2),

$$\alpha \equiv \xi^\nu\left[1 + \frac{\nu(\nu-1)}{1.2} + \ldots\right] \equiv 2^{\nu-1}\xi^\nu \pmod{p},$$

$$\beta \equiv \xi^{\nu-1}\left[\frac{\nu}{1} + \frac{\nu(\nu-1)(\nu-2)}{1.2.3} + \ldots\right] \equiv 2^{\nu-1}\xi^{\nu-1} \pmod{p},$$

ce qui montre que p ne peut diviser aucun des nombres α et β. Alors on pourra trouver deux entiers t et u, tels que l'on ait

$$(6) \qquad \alpha = \beta t + p^\nu u,$$

et en substituant cette valeur de α dans la formule (5), il viendra

$$\beta^2(t^2 - N) \equiv 0 \pmod{p^\nu},$$

ou

$$(7) \qquad t^2 - N \equiv 0 \pmod{p^\nu},$$

d'où il suit qu'on aura les deux racines de la congruence

proposée en prenant

$$x = \pm t.$$

Remarque. — Lorsque le nombre N est un multiple de p, cas que nous avons exclu, la congruence proposée exige que x soit divisible par p. Soit $N = p^{2n}N'$, n étant le degré de la plus haute puissance de p^2 qui divise N; la congruence proposée ne pourra être satisfaite que si x est divisible par p^n. Posant donc $x = p^n z$, elle se réduit à

$$z^2 - N' \equiv 0 \pmod{p^{\nu-2n}},$$

et celle-ci sera impossible ou n'aura que la racine $z = 0$, si N' contient encore le facteur p.

338. Considérons maintenant la congruence

$$x^2 - N \equiv 0 \pmod{2^\nu}.$$

Soit 2^{2n} la plus haute puissance de 2^2 qui divise N, il est évident que x doit avoir le diviseur 2^n; posant donc

$$N = 2^{2n}N', \quad x = 2^n z,$$

notre congruence deviendra

$$z^2 - N' \equiv 0 \pmod{2^{\nu-2n}}.$$

D'après cela on peut supposer que N soit impair ou double d'un impair. Si N est double d'un impair, il est évident que la proposée n'est résoluble que dans le seul cas de $\nu = 1$, et l'on peut faire abstraction de ce cas.

Soit donc N impair; si $\nu = 2$, la congruence proposée se réduit à

$$x^2 - 1 \equiv 0 \quad \text{ou à} \quad x^2 + 1 \equiv 0 \pmod{4};$$

la première est seule possible et n'a que les racines ± 1. Lorsque ν est > 2, la congruence proposée n'est possible que si N est de la forme $8k + 1$, et l'on obtient facilement

une solution par des substitutions successives. Il faut remarquer qu'une solution particulière conduit à la solution générale. Car soit x_0 une racine de la proposée, celle-ci pourra se mettre sous la forme

$$(x - x_0)(x + x_0) \equiv 0 \pmod{2^\nu};$$

d'où

$$x \pm x_0 = 2t, \quad x \mp x_0 = 2^{\nu-1} u,$$

t et u étant deux indéterminées. On tire de là

$$t = 2^{\nu-2} u \pm x_0;$$

u est arbitraire et les racines demandées sont données par la formule

$$x \equiv \pm x_0 + 2^{\nu-1} u \pmod{2^\nu}.$$

Exemple. — Soit la congruence

$$x^2 + 15 \equiv 0 \pmod{2^{10}},$$

la valeur $x = 1$ satisfait à la congruence prise suivant le module 2^4; on posera donc

$$x = 1 + 8x_1,$$

et, en substituant, il viendra

$$1 + x_1 + 4x_1^2 \equiv 0 \pmod{2^6}.$$

On voit que $1 + x_1$ doit être divisible par 4, et l'on fera en conséquence

$$x_1 = -1 + 4x_2,$$

ce qui donnera

$$1 - 7x_2 + 16x_2^2 \equiv 0 \pmod{2^4},$$

ou

$$1 - 7x_2 \equiv 0 \pmod{2^4};$$

cette dernière congruence est du premier degré et elle

a la racine 7; on fera donc

$$x_2 = 7,$$

et l'on en conclura $x_1 = 27$, $x = 217$. Les racines de la proposée seront ensuite données par la formule

$$x = \pm 217 + 512u,$$

qui comprend les quatre nombres

$$217, \quad 295, \quad 729, \quad 807.$$

339. Le cas général de la congruence

$$x^2 - N \equiv 0 \pmod{M},$$

suivant un module composé quelconque, se ramène aux cas précédents par un raisonnement déjà employé; car il est évident que tout nombre qui satisfait à la précédente congruence suivant le module

$$M = p^\nu q^\mu r^\lambda \ldots,$$

$p, q, r, \ldots$ étant des nombres premiers inégaux, satisfera à la même congruence suivant les modules p^ν, q^μ, r^λ, ... Ensuite si a, b, c, ... désignent des racines de ces congruences respectives, on aura l'une des solutions demandées, comme nous l'avons dit au n° 325, à l'occasion d'un cas semblable, en déterminant le nombre x de manière que l'on ait

$$x \equiv a \pmod{p^\nu}, \quad x \equiv b \pmod{q^\mu}, \quad x \equiv c \pmod{r^\lambda}, \ldots,$$

problème que nous savons résoudre.

CHAPITRE III.

PROPRIÉTÉS DES FONCTIONS ENTIÈRES D'UNE VARIABLE, RELATIVEMENT A UN MODULE PREMIER.

Des fonctions entières irréductibles, suivant un module premier.

340. Je me propose de présenter ici avec des développements entièrement nouveaux une théorie importante que j'ai déjà exposée dans la précédente édition de cet Ouvrage, en me plaçant à un point de vue un peu différent. Cette théorie se rapporte exclusivement aux modules premiers; elle a été l'objet d'un Mémoire présenté par moi à l'Académie des Sciences, le 4 décembre 1865.

Soient p un nombre premier, $\varphi(x)$ et $F(x)$ deux fonctions entières de x à coefficients entiers; si l'on peut trouver deux fonctions entières $\psi(x)$, $\chi(x)$ à coefficients entiers et qui soient telles que l'on ait identiquement

$$\varphi(x)\psi(x) = F(x) + p\chi(x),$$

et, par suite,

$$\varphi(x)\psi(x) \equiv F(x) \quad (\text{mod.}\ p),$$

nous dirons que la fonction $F(x)$ est *divisible par* $\varphi(x)$ *suivant le module* p, ou qu'elle est égale, *suivant le module* p, au produit des fonctions $\varphi(x)$, $\psi(x)$.

Supposons qu'une fonction entière $\varphi(x)$ soit ordonnée par rapport aux puissances décroissantes de x; si tous les coefficients sont divisibles par p, la fonction sera nulle suivant le module p; dans le cas contraire, soit a le premier des coefficients qui ne sont pas nuls suivant le mo-

dule p, on pourra trouver un entier α, tel que

$$a\alpha \equiv 1 \pmod{p},$$

et par conséquent le produit $\alpha\varphi(x)$ pourra se mettre sous la forme

$$\alpha\varphi(x) = F(x) + p\chi(x),$$

$F(x)$ désignant une fonction entière dans laquelle le coefficient de la plus haute puissance de x est l'unité; on peut évidemment supposer que tous les autres coefficients soient rabaissés au-dessous de p.

Une fonction entière $F(x)$ à coefficients entiers sera dite *irréductible suivant le module premier p*, si elle n'est divisible, suivant ce module, par aucune fonction entière d'un degré inférieur au sien et si, en outre, le coefficient de la plus haute puissance de x est égal à l'unité.

341. Théorème I. — *Si les deux fonctions $\varphi(x)$ et $\psi(x)$ n'admettent aucun diviseur commun, suivant le module premier p, on pourra trouver deux fonctions entières* U *et* V, *telles que l'on ait identiquement*

$$U\varphi(x) - V\psi(x) \equiv 1 \pmod{p}.$$

En effet, désignons par a et b les coefficients de la plus haute puissance de x dans $\varphi(x)$ et dans $\psi(x)$, on pourra poser

$$\varphi(x) \equiv aA, \quad \psi(x) \equiv bB \pmod{p},$$

A et B étant des fonctions entières dans lesquelles la plus haute puissance de x a pour coefficient l'unité.

Cela posé, exécutons sur les polynômes A et B l'opération par laquelle on détermine le plus grand commun diviseur, en négligeant les termes multipliés par p et en ayant soin d'ajouter à chaque reste un polynôme de la forme $p\lambda(x)$, choisi de manière qu'après cette addition le reste en question soit divisible par le coefficient du

et l'on a

$$\varphi(x) = F(x) f_1(x) + p\chi(x),$$

ou

$$\varphi(x) \equiv F(x) f_1(x) \pmod{p},$$

$f_1(x)$ étant une fonction entière.

Corollaire. — *Si la fonction entière* $F(x)$, *irréductible suivant le module premier p, ne divise suivant ce module aucune des fonctions* $\varphi_1(x), \varphi_2(x), \ldots, \varphi_m(x)$, *elle ne peut diviser la fonction*

$$\varphi(x) = \varphi_1(x)\varphi_2(x)\ldots\varphi_m(x) + p\chi(x)$$

congrue par rapport à p au produit des fonctions φ_1, $\varphi_2, \ldots, \varphi_m$.

Cette proposition se déduit immédiatement du théorème qu'on vient d'établir.

Remarques sur la décomposition d'une fonction entière en facteurs irréductibles.

343. Si une fonction entière $\varphi(x)$, non congrue à zéro suivant le module p, n'est pas irréductible, elle sera *décomposable en facteurs irréductibles;* en d'autres termes, on aura

$$F(x)F_1(x)F_2(x)\ldots F_{m-1}(x) = \alpha\varphi(x) + p\chi(x),$$

$F(x)$, $F_1(x)$, ... étant des polynômes à coefficients entiers, irréductibles suivant le module p, $\chi(x)$ une fonction entière et α le nombre par lequel il faut multiplier $\varphi(x)$ pour réduire à l'unité le coefficient de la plus haute puissance de x.

Il résulte du corollaire du théorème précédent que la fonction $\alpha\varphi(x)$ n'est décomposable suivant le module p

qu'en un seul système de facteurs irréductibles ; car supposons que l'on ait

$$ff_1f_2\ldots = FF_1F_2\ldots + p\chi(x),$$

les facteurs F et f étant supposés irréductibles. Le facteur irréductible F divise suivant le module p l'un des facteurs du premier membre, f par exemple, d'après le corollaire cité, et en conséquence il est congru à ce facteur, puisque celui-ci est lui-même irréductible. Remplaçant donc f par $F + p\chi(x)$, notre égalité prendra la forme

$$Ff_1f_2\ldots = FF_1F_2\ldots + p\chi(x)\,;$$

la fonction $\chi(x)$ doit être nécessairement divisible par F, et, en faisant la division, il vient

$$f_1f_2\ldots = F_1F_2\ldots + p\chi(x).$$

En poursuivant ce raisonnement, on voit que les facteurs F, F_1, F_2, ... sont respectivement égaux à f, f_1, f_2, ... suivant le module p.

344. Il peut arriver que plusieurs des facteurs irréductibles de la fonction $\alpha\varphi(x) = \Phi(x)$ soient égaux entre eux; dans ce cas, la fonction $\Phi(x)$ a un diviseur commun avec sa dérivée. Supposons que l'on ait

$$X_1^{n_1}X_2^{n_2}\ldots X_m^{n_m} = \Phi(x) + p\chi(x),$$

X_1, X_2, ..., X_m désignant des polynômes irréductibles suivant le module p et différents entre eux suivant ce module. Si l'on prend les dérivées des deux membres de cette égalité et qu'on représente par X'_i la dérivée de X_i, on aura

$$X_1^{n_1-1}X_2^{n_2-1}\ldots X_m^{n_m-1}(n_1X'_1X_2X_3\ldots X_m + \ldots + n_mX'_mX_1X_2\ldots X_{m-1})$$
$$= \Phi'(x) + p\chi'(x)\,;$$

si aucun des exposants n_1, n_2, ..., n_m n'est un multiple de p, le facteur entre parenthèses n'est divisible, suivant le module p, par aucun des facteurs irréductibles X_1, X_2, ..., X_m; car, pour qu'il fût divisible par X_1, par exemple, il faudrait que X_1 divisât l'un des facteurs du produit

$$X'_1 X_2 X_3 \ldots X_m;$$

or cela est impossible, puisque $X_2, X_3, \ldots, X_m$ sont irréductibles et différents de X_1, et que le degré de X'_1 est inférieur à celui de X_1. Le produit des facteurs irréductibles communs à $\Phi(x)$ et à sa dérivée est donc

$$X_1^{n_1-1} X_2^{n_2-1} \ldots X_m^{n_m-1};$$

c'est le *plus grand commun diviseur* de ces fonctions, suivant le module p, et pour l'obtenir on suivra la règle ordinaire en négligeant dans chaque division les multiples de p qui se présenteront, et en ayant soin de ramener à l'unité le coefficient du terme le plus élevé de chaque reste, avant de prendre celui-ci pour diviseur.

Si l'un des exposants, n_1 par exemple, est multiple de p, le facteur X_1 entrera à la puissance n_1 dans le plus grand commun diviseur.

Désignons par V_1 le produit de ceux des facteurs X_1, X_2, ... qui figurent dans $\Phi(x)$ avec un même exposant n_1, par V_2 le produit de ceux qui ont l'exposant n_2, et ainsi de suite; on aura

$$V_1^{n_1} V_2^{n_2} V_3^{n_3} \ldots = \Phi(x) + p\chi(x),$$

et, par un raisonnement identique à celui dont nous avons fait usage au n° 50, on prouvera que les facteurs V_1, V_2, V_3, ... peuvent être obtenus au moyen de simples divisions algébriques.

Des fonctions entières d'une variable, réduites suivant un module premier et suivant une fonction entière irréductible.

345. Si l'on divise une fonction entière $\mathfrak{F}(x)$ par un polynôme irréductible $F(x)$ d'un degré quelconque ν, on obtiendra un quotient $\varphi(x)$ et un reste qui pourra être représenté par $f(x)+p\,\chi(x)$, $f(x)$ étant une fonction entière du degré $\nu-1$ au plus dans laquelle les coefficients peuvent être pris, à volonté, entre les limites zéro et p ou entre $-\frac{p-1}{2}$ et $+\frac{p-1}{2}$. On aura ainsi

$$\mathfrak{F}(x)=f(x)+F(x)\varphi(x)+p\chi(x),$$

ou

$$\mathfrak{F}(x)\equiv f(x)+F(x)\varphi(x)\pmod{p}.$$

La fonction $f(x)$ sera dite la *valeur réduite de* $\mathfrak{F}(x)$, *suivant le module p et suivant la fonction irréductible* $F(x)$.

L'expression générale des fonctions réduites est

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_{\nu-1}x^{\nu-1};$$

chacun des coefficients a_0, a_1, ... étant susceptible de recevoir p valeurs différentes, par exemple

$$0,\ 1,\ 2,\ 3,\ldots,\ (p-1),$$

la fonction $f(x)$ peut avoir p^ν valeurs distinctes. Parmi ces valeurs il y en a p qui sont indépendantes de la variable x, ce sont les p nombres

$$0,\ 1,\ 2,\ 3,\ldots,\ (p-1).$$

THÉORÈME. — *Soient* $X_1, X_2, \ldots, X_m$ *m fonctions de x réduites, suivant le module p et suivant la fonc-*

tion entière irréductible $F(x)$. *Soit aussi*

$$\mathfrak{F}(X) = A_0X^m + A_1X^{m-1} + \ldots + A_{m-1}X + A_m$$

une fonction entière du degré m de la variable X, *dans laquelle les coefficients sont des fonctions entières de* x. *Si les résultats de la substitution de* $X_1, X_2, \ldots, X_m$ *à* X *dans* $\mathfrak{F}(X)$ *sont tous divisibles par* $F(x)$, *suivant le module* p, *on aura identiquement*

$$\begin{aligned}\mathfrak{F}(X) = A_0(X - X_1)(X - X_2)\ldots(X - X_m)\\ + F(x)\,\varphi(X, x) + p\,\chi(X, x),\end{aligned}$$

φ *et* χ *étant des fonctions entières, à coefficients entiers, des deux variables* x *et* X.

En effet, regardant $X_1, X_2, \ldots, X_m$ comme des indéterminées, désignons par $\mathfrak{F}_1(X)$ et R_1 le quotient et le reste de la division de $\mathfrak{F}(X)$ par $X - X_1$; soient de même $\mathfrak{F}_2(X)$ et R_2 le quotient et le reste de la division de $\mathfrak{F}_1(X)$ par $X - X_2$, et ainsi de suite; en sorte que $\mathfrak{F}_m(X)$ et R_m exprimeront le quotient et le reste de la dernière division, savoir celle de $\mathfrak{F}_{m-1}(X)$ par $X - X_m$. Les égalités

$$(1)\quad \left\{\begin{aligned}\mathfrak{F}(X) &= (X - X_1)\,\mathfrak{F}_1(X) + R_1,\\ \mathfrak{F}_1(X) &= (X - X_2)\,\mathfrak{F}_2(X) + R_2,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ \mathfrak{F}_{m-1}(X) &= (X - X_m)\,\mathfrak{F}_m(X) + R_m\end{aligned}\right.$$

donneront, à cause de $\mathfrak{F}_m(X) = A_0$,

$$(2)\quad \left\{\begin{aligned}\mathfrak{F}(X) = R_1 + R_2(X - X_1) + R_3(X - X_1)(X - X_2) + \ldots\\ + R_m(X - X_1)\ldots(X - X_{m-1})\\ + A_0(X - X_1)\ldots(X - X_m),\end{aligned}\right.$$

et, si l'on remplace X successivement par $X_1, X_2, \ldots,$

X_m, il viendra

$$(3)\quad \begin{cases} \mathfrak{F}(X_1) = R_1, \\ \mathfrak{F}(X_2) = R_1 + R_2(X_2 - X_1), \\ \mathfrak{F}(X_3) = R_1 + R_2(X_3 - X_1) + R_3(X_3 - X_1)(X_3 - X_2), \\ \dots\dots\dots\dots\dots\dots, \\ \mathfrak{F}(X_m) = R_1 + R_2(X_m - X_1) + \dots \\ \qquad\qquad + R_m(X_m - X_1)\dots(X_m - X_{m-1}). \end{cases}$$

Supposons maintenant que $X_1, X_2, \dots, X_m$ désignent des fonctions entières de x réduites, suivant le module p et suivant la fonction irréductible $F(x)$. Si ces fonctions sont distinctes, aucune de leurs différences deux à deux ne pourra être divisible par $F(x)$, suivant le module p, et comme les premiers membres des formules (3) le sont, par hypothèse, les polynômes R_1, R_2, ..., R_m seront eux-mêmes divisibles par $F(x)$, suivant le module p. Alors la formule (2) prendra la forme

$$(4)\quad \begin{cases} \mathfrak{F}(X) = A_0(X - X_1)\dots(X - X_m) \\ \qquad\qquad + F(x)\varphi(X, x) + p\chi(X, x), \end{cases}$$

conformément à l'énoncé du théorème.

Corollaire. — *Soit $\mathfrak{F}(X)$ une fonction entière des deux variables X et x, du degré m par rapport à X, et dans laquelle le coefficient de X^m n'est pas divisible, suivant le module p, par la fonction irréductible $F(x)$; si l'on substitue successivement à X les p^ν fonctions de x réduites suivant le module p, et suivant la fonction $F(x)$, parmi les p^ν résultats obtenus il y en aura m au plus qui seront divisibles par $F(x)$ suivant le module p.*

En effet, supposons les m fonctions de x,

$$X_1,\ X_2,\ \dots,\ X_m$$

réduites, suivant le module p et suivant la fonction $F(x)$, telles que

$$\mathfrak{F}(X_1),\ \mathfrak{F}(X_2),\ \dots,\ \mathfrak{F}(X_m)$$

soient divisibles par $F(x)$ suivant le module p. Alors la formule (4) aura lieu identiquement, et, si l'on y remplace X par une fonction réduite X_{m+1} distincte de X_1, X_2, ..., X_m, on aura

$$\mathfrak{F}(X_{m+1}) = A_0(X_{m+1} - X_1)\ldots(X_{m+1} - X_m)$$
$$- F(x)\varphi(x) + p\chi(x).$$

Or $F(x)$ ne peut diviser suivant le module p le produit des différences $X_{m+1} - X_1$, $X_{m+1} - X_2$, ...; donc $\mathfrak{F}(X_{m+1})$ n'est pas divisible, suivant le module, par le polynôme $F(x)$.

Propriétés fondamentales des polynômes irréductibles suivant un module premier.

346. Théorème I. — *Tout polynôme* $F(x)$ *à coefficients entiers et du degré* ν, *irréductible suivant le module premier* p, *divise, suivant ce module, la fonction* $x^{p^\nu} - x$.

L'expression générale des fonctions entières de x réduites, suivant le module p et suivant la fonction irréductible $F(x)$, est

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{\nu-1} x^{\nu-1},$$

a_0, a_1, ..., $a_{\nu-1}$ étant des entiers compris entre zéro et $p-1$, ou entre $-\frac{p-1}{2}$ et $+\frac{p-1}{2}$. L'une de ces fonctions est nulle : nous en ferons abstraction et nous désignerons par

$$(1) \qquad X_1,\ X_2,\ X_3,\ \ldots,\ X_{p^\nu-1}$$

les $p^\nu - 1$ fonctions réduites différentes de zéro.

Cela posé, désignons par $f(x)$ une fonction entière

de x non divisible par $F(x)$, suivant le module p, et considérons les produits des fonctions (1) par $f(x)$, savoir

$$(2) \qquad X_1 f(x),\ X_2 f(x), \ldots,\ X_{p^\nu-1} f(x).$$

Aucun de ces produits n'est divisible, suivant le module p, par le polynôme irréductible $F(x)$, puisque les facteurs qui le composent n'admettent pas ce diviseur : la différence de deux termes de la suite (2) ne peut elle-même être divisible par $F(x)$, suivant le module p, car cette différence est évidemment un terme de la suite (2). Si donc on prend les valeurs réduites des produits (2), suivant le module p et suivant le polynôme irréductible $F(x)$, ces valeurs seront distinctes et aucune d'elles ne sera zéro ; en conséquence, elles coïncideront, abstraction faite de l'ordre, avec les termes de la suite (1). Il résulte de là qu'il existe entre les fonctions de la suite (2) et leurs correspondantes de la suite (1) $p^\nu - 1$ congruences de la forme

$$X_m f(x) \equiv X_n + F(x)\varphi(x) \pmod{p},$$

et si l'on multiplie entre elles toutes ces congruences, il viendra

$$X_1 X_2 \ldots X_{p^\nu-1}\left[f(x)^{p^\nu-1} - 1\right] \equiv F(x)\varphi(x) \pmod{p},$$

$\varphi(x)$ étant une fonction entière. Le produit $X_1 X_2 \ldots X_{p^\nu-1}$ n'est pas divisible par $F(x)$, suivant le module p ; donc on a

$$(3) \qquad f(x)^{p^\nu-1} - 1 \equiv F(x)\varphi(x) \pmod{p},$$

ou, en multipliant par $f(x)$,

$$(4) \qquad f(x)^{p^\nu} - f(x) \equiv F(x)\varphi(x) \pmod{p}.$$

Nous avons supposé la fonction $f(x)$ non divisible par

$F(x)$ suivant le module p, mais il est évident que la formule (4) subsiste quand $f(x)$ est un multiple de $F(x)$.

La formule (4) ayant lieu, quelle que soit la fonction entière $f(x)$, prenons $f(x) = x$, il viendra

(5) $$x^{p^\nu} - x \equiv F(x)\varphi(x) \pmod{p},$$

ce qui démontre le théorème énoncé.

347. Lemme. — *Soient $f(x)$ une fonction entière de la variable x, p un nombre premier et n un nombre entier quelconque; on a*

$$f(x^{p^n}) = [f(x)]^{p^n} + p\chi(x),$$

$\chi(x)$ désignant une fonction entière.

Soit

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_m x^m;$$

la puissance $p^{\text{ième}}$ de $f(x)$ renfermera d'abord les puissances $p^{\text{ièmes}}$ des différents termes; elle renfermera en outre d'autres termes contenant certaines puissances de plusieurs termes de $f(x)$: le coefficient de l'un quelconque de ces derniers termes aura la forme

$$\frac{1.2\ldots p}{(1.2\ldots q_1)\ldots(1.2\ldots q_k)},$$

$q_1, q_2, \ldots, q_k$ étant des nombres inférieurs à p; ce coefficient est donc divisible par p et l'on a

$$[f(x)]^p + p\chi(x) = a_0^p + a_1^p x^p + a_2^p x^{2p} + \dots + a_m^p x^{mp};$$

mais, par le théorème de Fermat, on a

$$a^p \equiv a \pmod{p};$$

donc

$$[f(x)]^p + p\chi(x) = a_0 + a_1 x^p + a_2 x^{2p} + \dots + a_m x^{mp}$$

ou

$$f(x^p) = [f(x)]^p + p\chi(x),$$

$\chi(x)$ étant une fonction entière.

Si l'on écrit $x^{p^{n-1}}$ au lieu de x, il vient

$$f(x^{p^n}) = [f(x^{p^{n-1}})]^p + p\chi(x),$$

$\chi(x)$ désignant ici une nouvelle fonction entière. Cela posé, admettons que l'on ait

$$f(x^{p^{n-1}}) = [f(x)]^{p^{n-1}} + p\chi(x);$$

en élevant cette égalité à la puissance p, et ayant égard à la précédente, il vient

$$f(x^{p^n}) = [f(x)]^{p^n} + p\chi(x).$$

Donc, si cette dernière égalité a lieu pour une valeur de l'exposant n, elle a lieu pour la valeur immédiatement supérieure; d'ailleurs elle a été démontrée pour $n = 1$, donc elle est générale.

348. Théorème II. — *Une fonction entière* $F(x)$ *du degré* ν, *irréductible suivant le module premier* p, *ne divise la fonction* $x^{p^\mu} - x$, *suivant ce même module, que dans le cas où* μ *est un multiple de* ν.

Je dis en premier lieu que, si l'on a $\mu < \nu$, la fonction $x^{p^\mu} - x$ n'est pas divisible par $F(x)$ suivant le module p, c'est-à-dire qu'on ne peut avoir

(1) $$x^{p^\mu} - x = F(x)\varphi(x) + p\chi(x),$$

$\varphi(x)$ et $\chi(x)$ étant des polynômes à coefficients entiers. Admettons, en effet, que cette égalité (1) ait lieu, et posons

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{\nu-1} x^{\nu-1},$$

$a_0, a_1, \ldots$ étant des entiers quelconques compris entre

zéro et $p-1$. On aura, d'après le lemme qui précède,

$$[f(x)]^{p^\mu} = f(x^{p^\mu}) + p\chi_1(x),$$

$\chi_1(x)$ étant une fonction entière, et si, dans le second membre de cette identité, on remplace x^{p^μ} par la valeur $x + F(x)\varphi(x) + p\chi(x)$ tirée de la formule (1), il est évident que ce second membre prendra la forme

$$f(x) + F(x)\Phi(x) + p\Psi(x),$$

Φ et Ψ étant des polynômes à coefficients entiers; on aura donc

$$(2) \qquad [f(x)]^{p^\mu} - f(x) = F(x)\Phi(x) + p\Psi(x).$$

Il résulte de cette formule (2) que si, dans la fonction

$$X^{p^\mu} - X,$$

qui est du degré p^μ, on remplace X par chacune des p^ν fonctions réduites suivant le module p, et la fonction $F(x)$, on obtient p^ν résultats qui sont tous divisibles par $F(x)$, suivant le module p. Or cela est impossible (nº 345) si $\mu < \nu$; donc la formule (1) ne peut avoir lieu dans ce cas.

Je dis, en second lieu, que la formule (1) ne peut avoir lieu que si μ est divisible par ν. En effet, soit q le quotient et r le reste de la division de μ par ν, en sorte qu'on ait

$$\mu = \nu q + r.$$

D'après le théorème I (nº 346), $F(x)$ divise, suivant le module p, la fonction

$$x^{p^\nu} - x = x\left[x^{p^\nu - 1} - 1\right],$$

et celle-ci divise *algébriquement*

$$x(x^{p^{\nu q}-1} - 1) = x^{p^{\nu q}} - x,$$

car l'exposant $p^{\nu q} - 1$ est un multiple de $p^\nu - 1$. Donc $x^{p^{\nu q}} - x$ est divisible, suivant le module p, par $F(x)$. Mais, par hypothèse, la fonction $x^{p^\mu} - x$ est elle-même divisible par $F(x)$, suivant le module p; donc il en sera de même de la différence

$$(x^{p^\mu} - x) - (x^{p^{\nu q}} - x) = x^{p^{\nu q + r}} - x^{p^{\nu q}};$$

d'après le lemme du n° 347, cette différence est congrue, suivant le module p, à la puissance

$$(x^{p^r} - x)^{p^{\nu q}}$$

et cette puissance ne peut être divisible par $F(x)$ suivant le module p, à moins que

$$x^{p^r} - x$$

ne le soit elle-même. Or cela ne peut être, comme on l'a vu plus haut, que si $r = 0$, puisque r est inférieur à ν.

Détermination du nombre des fonctions entières de degré ν irréductibles suivant un module premier p.

349. Nous sommes actuellement en mesure d'établir qu'il existe, dans chaque degré ν, des fonctions entières irréductibles suivant un module premier p; il est même facile, comme on va le voir, de déterminer le nombre de ces fonctions.

Considérons la fonction $x^{p^\nu} - x$, et supposons-la décomposée en facteurs irréductibles suivant le module premier p, de manière qu'on ait

$$F(x) F_1(x) F_2(x) \ldots = x^{p^\nu} - x + p\chi(x),$$

$F(x)$, $F_1(x)$, $F_2(x)$, ... étant des fonctions entières irréductibles suivant le module p, et $\chi(x)$ une fonction entière quelconque.

Deux des facteurs F, F_1, F_2, ... ne sauraient être égaux entre eux, puisque la fonction $x^{p^\nu}-x$ n'a aucun facteur commun avec sa dérivée. En outre, les développements que nous avons présentés plus haut conduisent aux conséquences suivantes :

1° Toute fonction entière de degré ν, irréductible suivant le module premier p, fait partie de la suite $F(x)$, $F_1(x)$, $F_2(x)$, ...

2° Le degré de l'une quelconque des fonctions de cette suite est égal à ν ou un diviseur de ν.

3° Celles des fonctions $F(x)$, $F_1(x)$, $F_2(x)$, ..., dont le degré est un diviseur μ de ν inférieur à ν, sont diviseurs, suivant le module p, de la fonction $x^{p^\mu}-x$.

Il résulte de là que si l'on divise la fonction $x^{p^\nu}-x$, suivant le module p, par le produit de toutes les fonctions irréductibles qui divisent l'une des fonctions $x^{p^\mu}-x$, où μ est un diviseur de ν, on obtiendra un quotient V qui sera le produit de toutes les fonctions entières de degré ν, irréductibles suivant le module p.

Par exemple, si ν est un nombre premier, les facteurs irréductibles de $x^{p^\nu}-x$ sont tous du degré ν ou du degré 1 ; le produit des facteurs du premier degré est $x(x-1)(x-2)\ldots(x-p+1)$ ou x^p-x. On aura donc, dans ce cas,

$$V=\frac{x^{p^\nu}-x}{x^p-x};$$

le degré de V est ici $p^\nu-p$; par conséquent, *le nombre* N *des fonctions entières d'un degré premier ν, irréductibles suivant un module premier p, est*

$$N=\frac{p^\nu-p}{\nu}.$$

Passons maintenant au cas général : soit

$$\nu=q_1^{n_1}q_2^{n_2}\ldots q_m^{n_m},$$

$q_1, q_2, \ldots, q_m$ étant des nombres premiers inégaux, et $n_1, n_2, \ldots, n_m$ des entiers positifs quelconques. Pour abréger l'écriture, je poserai, quel que soit l'entier λ,

$$x^{p^\lambda} - x = [\lambda];$$

et je ferai en outre

$$\begin{aligned} X &= [\nu],\\ X_1 &= \left[\frac{\nu}{q_1}\right]\left[\frac{\nu}{q_2}\right]\cdots\left[\frac{\nu}{q_m}\right],\\ X_2 &= \left[\frac{\nu}{q_1 q_2}\right]\left[\frac{\nu}{q_1 q_3}\right]\cdots\left[\frac{\nu}{q_{m-1} q_m}\right],\\ &\ldots\ldots\ldots\ldots\ldots\ldots,\\ X_m &= \left[\frac{\nu}{q_1 q_2 \ldots q_m}\right]; \end{aligned}$$

la fonction X_k sera ainsi le produit de

$$\frac{m(m-1)\ldots(m-k+1)}{1.2\ldots k}$$

symboles [ ], et les dénominateurs des arguments de ces symboles seront les produits k à k des m nombres q_1, $q_2, \ldots, q_m$. Cela posé, je dis que l'on aura

$$V = \frac{X X_2 X_4 X_6 \ldots}{X_1 X_3 X_5 \ldots}.$$

Concevons que le numérateur et le dénominateur de cette expression aient été décomposés en facteurs irréductibles, et désignons par $F(x)$ l'un de ces facteurs. Si $F(x)$ est du degré ν, il ne figurera que dans X; par suite il aura l'exposant 1 dans le numérateur de l'expression précédente, et le degré zéro dans le dénominateur.

Supposons que le degré μ de $F(x)$ soit inférieur à ν; quelques-uns des facteurs premiers q entreront dans ν au moins une fois de plus que dans μ; si l'on désigne par

$q_1, q_2, \ldots, q_s$ ces facteurs, dont le nombre s peut se réduire à 1, le degré μ divisera $\frac{\nu}{q_1 q_2 \ldots q_s}$, mais il ne divisera pas le quotient de ν par un nouveau facteur q, tel que q_{s+1}. Le facteur irréductible $F(x)$ figure dans X à la première puissance; cherchons généralement avec quel exposant il se trouve dans X_k. Si l'on a $k > s$, la fonction X_k ne contient pas le facteur $F(x)$; mais, si l'on a $k < s$ ou $k = s$, il est évident que X_k contiendra autant de facteurs égaux à $F(x)$ qu'il y a d'unités dans le nombre des combinaisons de s lettres prises k à k, nombre qui a pour valeur $\frac{s(s-1)\ldots(s-k+1)}{1.2\ldots k}$; par conséquent, le numérateur et le dénominateur de l'expression précédente contiendront le facteur $F(x)$ avec des exposants qui seront respectivement égaux à

$$1 + \frac{s(s-1)}{1.2} + \frac{s(s-1)(s-2)(s-3)}{1.2.3.4} + \ldots$$

et

$$\frac{s}{1} + \frac{s(s-1)(s-2)}{1.2.3} + \frac{s(s-1)\ldots(s-4)}{1.2.3.4.5} + \ldots.$$

Mais ces deux nombres sont égaux, car leur différence est évidemment égale à $(1-1)^s$ ou à zéro. Donc le numérateur de notre expression est divisible, suivant le module p, par le dénominateur, et le quotient de la division est bien égal au produit V de toutes les fonctions entières de degré ν, irréductibles suivant le module p.

Il convient au reste de remarquer que le numérateur de l'expression de V est *algébriquement* divisible par le dénominateur; et, pour démontrer ce fait, il suffit de reproduire le raisonnement dont nous venons de faire usage, en représentant toujours par μ un diviseur de ν et en substituant au polynôme $F(x)$ de degré μ l'un des

facteurs linéaires qui divisent algébriquement $x^{p^\mu} - x$, mais qui ne divisent pas $x^{p^{\mu_1}} - x$, μ_1 étant $< \mu$.

Le degré du polynôme V peut être représenté par

$$p^\nu - \sum p^{\frac{\nu}{q_1}} + \sum p^{\frac{\nu}{q_1 q_2}} - \ldots + (-1)^{m-1} \sum p^{\frac{\nu}{q_1 q_2 \ldots q_{m-1}}} + (-1)^m p^{\frac{\nu}{q_1 q_2 \ldots q_m}},$$

et, puisque ce polynôme est le produit de toutes les N fonctions entières de degré ν, irréductibles suivant le module p, on aura

$$N = \frac{p^\nu - \sum p^{\frac{\nu}{q_1}} + \sum p^{\frac{\nu}{q_1 q_2}} - \ldots + (-1)^{m-1} \sum p^{\frac{\nu}{q_1 q_2 \ldots q_{m-1}}} + (-1)^m p^{\frac{\nu}{q_1 q_2 \ldots q_m}}}{\nu}.$$

350. On peut conclure de la formule précédente deux limites très-simples du nombre N des congruences irréductibles de degré ν, suivant le module premier p. Effectivement, en partant de la formule

$$p^t = 1 + \frac{t \log p}{1} + \frac{t^2 \log^2 p}{1.2} + \ldots,$$

on aura

$$\begin{aligned} N = & \left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_m}\right) \frac{\log p}{1} \\ & + \left(1 - \frac{1}{q_1^2}\right)\left(1 - \frac{1}{q_2^2}\right) \cdots \left(1 - \frac{1}{q_m^2}\right) \frac{\nu \log^2 p}{1.2} \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & + \left(1 - \frac{1}{q_1^k}\right)\left(1 - \frac{1}{q_2^k}\right) \cdots \left(1 - \frac{1}{q_m^k}\right) \frac{\nu^{k-1} \log^k p}{1.2\ldots k} \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{aligned}$$

la caractéristique log exprimant des logarithmes népériens.

On conclut d'abord de cette formule

$$N < \left(1 - \frac{1}{\nu}\right)\frac{\log p}{1} + \left(1 - \frac{1}{\nu^2}\right)\frac{\nu \log^2 p}{1.2} + \left(1 - \frac{1}{\nu^3}\right)\frac{\nu^2 \log^3 p}{1.2.3} + \ldots,$$

ou

$$N < \frac{p^\nu - p}{\nu},$$

puis

$$N > \frac{\varphi(\nu)}{\nu}\left(\frac{\log p}{1} + \frac{1-\frac{1}{\nu^2}}{1-\frac{1}{\nu}}\frac{\nu\log^2 p}{1.2} + \frac{1-\frac{1}{\nu^3}}{1-\frac{1}{\nu}}\frac{\nu^2\log^3 p}{1.2.3} + \ldots\right)$$

ou

$$N > \frac{\varphi(\nu)}{\nu - 1}\,\frac{p^\nu - p}{\nu},$$

$\varphi(\nu)$ désignant la totalité des nombres premiers et inférieurs à ν. Chacune des limites que nous venons de trouver exprime la valeur de N quand ν est un nombre premier.

Sur la décomposition d'une fonction entière donnée, en facteurs irréductibles suivant un module premier.

351. S'il s'agit de décomposer une fonction donnée $\mathfrak{F}(x)$ en facteurs irréductibles suivant le module premier p, on devra d'abord chercher si cette fonction a des diviseurs multiples; car, si elle en admet, elle sera de la forme

$$\mathfrak{F}(x) \equiv V_1^{n_1} V_2^{n_2} V_3^{n_3} \ldots \quad (\text{mod.}\, p),$$

V_1, V_2, ... étant des fonctions entières qui n'admettent que des facteurs simples et que l'on peut obtenir (n° 344) par de simples divisions algébriques.

La question est donc ramenée au cas où $\mathfrak{F}(x)$ n'a que des facteurs simples; alors cette fonction et sa dérivée n'ont aucun diviseur commun, suivant le module p.

Cela posé, on aura le produit des facteurs irréductibles du premier degré de $\mathfrak{F}(x)$ en cherchant le plus grand

commun diviseur des polynômes $\mathfrak{F}(x)$ et $x^p - x$; désignons par P_1 ce plus grand commun diviseur qui peut se réduire à l'unité et posons

$$\mathfrak{F}(x) \equiv P_1 \mathfrak{F}_1(x) \quad (\text{mod}. p),$$

$\mathfrak{F}_1(x)$ étant une fonction entière.

On aura de même le produit des facteurs irréductibles du deuxième degré de $\mathfrak{F}(x)$ ou de $\mathfrak{F}_1(x)$, en cherchant le plus grand commun diviseur des polynômes $\mathfrak{F}_1(x)$ et $x^{p^2} - x$, et si P_2 désigne ce plus grand commun diviseur, lequel peut encore être égal à 1, on aura

$$\mathfrak{F}_1(x) \equiv P_2 \mathfrak{F}_2(x) \quad (\text{mod}. p),$$

$\mathfrak{F}_2(x)$ étant une fonction entière.

Pareillement, le plus grand commun diviseur P_3 des fonctions $\mathfrak{F}_2(x)$ et $x^{p^3} - x$ donnera, s'il ne se réduit pas à 1, le produit des diviseurs du troisième degré; on aura

$$\mathfrak{F}_2(x) \equiv P_3 \mathfrak{F}_3(x) \quad (\text{mod}. p),$$

et ainsi de suite. Il est évident qu'en continuant ainsi on trouvera nécessairement une fonction $\mathfrak{F}_m(x)$ qui se réduira à l'unité, et l'on aura

$$\mathfrak{F}(x) \equiv P_1 P_2 P_3 \ldots P_m \quad (\text{mod}. p).$$

Il reste, pour achever la solution, à décomposer chacun des polynômes P_ν en facteurs irréductibles du degré ν. Pour cela, la méthode la plus générale consiste à effectuer la division du polynôme P_ν par la fonction

$$F(x) = x^\nu + A_1 x^{\nu-1} + A_2 x^{\nu-2} + \ldots + A_{\nu-1} x + A_\nu$$

dans laquelle les coefficients sont indéterminés, et à exprimer que les ν termes du reste sont congrus à zéro suivant le module p. On obtiendra ainsi un système de ν congruences au moyen desquelles on pourra déterminer

les ν coefficients $A_1, A_2, \ldots, A_\nu$. Si $\mu\nu$ désigne le degré de la fonction P_ν, il est évident que le système de congruences dont il vient d'être question admettra μ systèmes de solutions qui répondront respectivement aux μ polynômes irréductibles de degré ν dont le produit est égal à P_ν.

Le problème dont nous venons de nous occuper comprend comme cas particulier celui qui a pour objet la recherche de toutes les fonctions entières de degré ν, irréductibles suivant le module p. On tombe effectivement sur ce dernier problème, en supposant dans ce qui précède

$$\mathfrak{F}(x) = x^{p^\nu} - x.$$

Classification des fonctions entières de degré ν irréductibles suivant le module premier p.

352. Soit n un diviseur de $p^\nu - 1$, la fonction $x^n - 1$ divisera $x^{p^\nu - 1} - 1$ et $x^{p^\nu} - x$; si donc on la décompose en facteurs irréductibles, suivant le module p, en sorte qu'on ait

$$F(x)\,F_1(x)\,F_2(x)\ldots = x^n - 1 + p\chi(x),$$

$\chi(x)$ étant une fonction entière, les fonctions $F(x)$, $F_1(x)$, ... feront partie de la suite des facteurs irréductibles de $x^{p^\nu} - x$, et en conséquence leur degré sera égal à ν ou à un diviseur de ν.

Si $F(x)$ est une fonction entière du degré ν, irréductible suivant le module p, et que n représente le plus petit nombre tel que $x^n - 1$ soit divisible par $F(x)$ suivant le module p, je dirai que *la fonction* $F(x)$ *appartient à l'exposant* n. Il est évident que n est un diviseur de $p^\nu - 1$, car $F(x)$ divisant, suivant le module p, les deux fonctions $x^{p^\nu - 1} - 1$ et $x^n - 1$, elle divisera aussi $x^\delta - 1$,

si l'on désigne par θ le plus grand commun diviseur des nombres $p^\nu - 1$ et n, et puisque $F(x)$ appartient à l'exposant n, il est nécessaire que l'on ait $\theta = n$. On voit aussi que n doit être un *diviseur propre* à $p^\nu - 1$, c'est-à-dire que n ne peut diviser $p^\mu - 1$ si μ est $< \nu$; car s'il en était autrement $x^n - 1$ serait un diviseur de $x^{p^\mu - 1} - 1$ et cette dernière fonction serait par suite divisible par $F(x)$ suivant le module p, ce qui est impossible dans l'hypothèse de $\mu < \nu$.

Cela posé, nous nous proposons de déterminer le nombre des fonctions entières de degré ν, irréductibles suivant le module premier p, et qui appartiennent à l'exposant n diviseur propre de $p^\nu - 1$.

Le nombre n étant décomposé en facteurs premiers, soit

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_m^{\alpha_m},$$

$q_1, q_2, \ldots, q_m$ étant des nombres premiers inégaux; posons aussi

$$X = x^n - 1,$$

$$X_1 = \left(x^{\frac{n}{q_1}} - 1\right)\left(x^{\frac{n}{q_2}} - 1\right)\ldots\left(x^{\frac{n}{q_m}} - 1\right),$$

$$X_2 = \left(x^{\frac{n}{q_1 q_2}} - 1\right)\left(x^{\frac{n}{q_1 q_3}} - 1\right)\ldots\left(x^{\frac{n}{q_{m-1} q_m}} - 1\right),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$X_m = \left(x^{\frac{n}{q_1 q_2 \ldots q_m}} - 1\right),$$

la fonction X_k sera, comme on voit, le produit de $\frac{m(m-1)\ldots(m-k+1)}{1.2\ldots k}$ facteurs qui se déduiront de $x^{\frac{n}{\theta_k}} - 1$ en prenant pour θ_k les produits k à k des facteurs $q_1, q_2, \ldots, q_m$. Si l'on désigne enfin par V le produit de toutes les fonctions entières de degré ν, irréductibles

suivant le module p, et qui appartiennent à l'exposant n, je dis que l'on aura

$$V = \frac{XX_2X_4X_6\ldots}{X_1X_3X_5\ldots}.$$

Pour justifier cette assertion nous emploierons un raisonnement semblable à celui dont nous avons fait usage au nº 349. Les deux termes de l'expression de V étant décomposés en facteurs irréductibles, soit $F(x)$ l'un de ces facteurs; si la fonction $F(x)$ appartient à l'exposant n, elle ne figurera que dans X; en conséquence, elle aura l'exposant 1 au numérateur de V et l'exposant zéro au dénominateur. Si la fonction $F(x)$ appartient à un exposant m inférieur à n, m divisera les quotients obtenus en divisant n par quelques-uns des facteurs $q, q_1, q_2, \ldots, q_s$ par exemple; le facteur $F(x)$ figure dans X à la première puissance; il ne figure point dans X_k si l'on a $k > s$; mais si l'on a $k < s$, $F(x)$ entrera dans X_k avec l'exposant $\frac{s(s-1)\ldots(s-k+1)}{1.2\ldots k}$, qui est égal au nombre des combinaisons de s lettres prises k à k. Il résulte de là que, quand on aura simplifié l'expression de V, le facteur $F(x)$ aura l'exposant

$$1 - \frac{s}{1} + \frac{s(s-1)}{1.2} - \ldots = (1-1)^s = 0,$$

et, en conséquence, la fonction V est égale au produit de toutes les fonctions irréductibles de degré ν, qui appartiennent à l'exposant n; nous désignerons par N le nombre de ces fonctions.

Le degré de la fonction V est

$$n - \left(\frac{n}{q_1} + \frac{n}{q_2} + \ldots + \frac{n}{q_m}\right) + \left(\frac{n}{q_1q_2} + \frac{n}{q_1q_3} + \ldots\right) - \ldots$$
$$\pm \frac{n}{q_1q_2\ldots q_m}$$

ou

$$n\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_m}\right);$$

on aura donc

$$N=\frac{1}{\nu}n\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_m}\right),$$

ou

$$N=\frac{\varphi(n)}{\nu},$$

en désignant par $\varphi(n)$ le nombre des entiers inférieurs à n et premiers à n.

Si n est un nombre premier, la formule précédente se réduit à

$$N=\frac{n-1}{\nu},$$

et l'on en tire

$$n=\nu N+1,$$

d'où il résulte que tout nombre premier, diviseur propre à $p^\nu-1$, est de la forme $k\nu+1$, ce qui rentre dans un théorème dû à Euler.

353. On voit, par ce qui précède, que les fonctions entières de degré ν, irréductibles suivant le module p, se partagent naturellement en plusieurs classes, d'après l'exposant auquel elles appartiennent. L'une de ces classes comprend les fonctions qui appartiennent à l'exposant $p^\nu-1$ et qui jouent un rôle important dans la théorie que nous exposons; on a, par exemple, la propriété remarquable comprise dans le théorème suivant :

Théorème. — *Si* $F(x)$ *désigne une fonction de degré* ν, *irréductible suivant le module* p, *et appartenant à l'exposant* $p^\nu-1$, *on obtiendra les* $p^\nu-1$ *fonctions entières de degré* $\nu-1$ *distinctes suivant le module* p,

en prenant les restes de la division par $F(x)$ *des puissances*

$$x,\ x^2,\ x^3,\ldots,\ x^{p^\nu-1}.$$

En effet, deux de ces puissances, x^m et x^{n+m}, divisées par $F(x)$, ne peuvent donner des restes de degrés $\nu-1$ congrus suivant le module p; car autrement l'expression

$$x^{n+m}-x^m \quad \text{ou} \quad x^m(x^n-1)$$

serait divisible par $F(x)$ suivant le module p, et il en serait de même de x^n-1 : or cela est impossible, puisque n est moindre que l'exposant $p^\nu-1$ auquel appartient $F(x)$.

354. J'indiquerai ici une conséquence assez remarquable de la théorie que nous venons d'exposer et qui consiste dans la proposition suivante :

Théorème. — *Si n est un nombre premier, que a soit une racine primitive de n, et que le module p soit de la forme $a+kn$, la fonction*

$$V=\frac{x^n-1}{x-1}$$

sera irréductible suivant le module p.

En effet, n est un nombre premier; il est d'ailleurs diviseur propre à $p^{n-1}-1$, puisque $p-kn$ est une racine primitive de n; donc le nombre des facteurs irréductibles de V, suivant le module p, est ici égal à $\frac{\varphi(n)}{n-1}$ ou à 1.

Corollaire. — *Si n est premier, la fonction $\frac{x^n-1}{x-1}$ est* algébriquement *irréductible.*

En effet, soit a une racine primitive de n. L'illustre Lejeune-Dirichlet a prouvé que la progression arithmétique

$$a,\ a+n,\ a+2n,\ a+3n,\ \ldots$$

renferme une infinité de nombres premiers. Soit

$$p = a + kn$$

l'un de ces nombres premiers; la fonction $\frac{x^n - 1}{x - 1}$ est irréductible suivant le module p; donc, à plus forte raison, elle est irréductible *algébriquement*.

Comparaison des fonctions entières irréductibles suivant le module p, qui appartiennent à des exposants formés des mêmes facteurs premiers.

355. Lorsque n est divisible par le module p, si l'on fait $n = pn'$, on aura

$$x^n - 1 \equiv (x^{n'} - 1)^p \pmod{p},$$

en sorte que la fonction $x^n - 1$ est ramenée à $x^{n'} - 1$.

Nous supposerons que n n'est pas divisible par p; alors, si l'on désigne par ν le plus petit nombre tel, que $p^\nu - 1$ soit divisible par n, la fonction $x^n - 1$ divisera $x^{p^\nu} - x$ suivant le module p et chacun de ses facteurs irréductibles sera, comme on l'a vu, d'un degré égal à ν ou à un diviseur de ν. Mais ceux de ces facteurs qui appartiennent à l'exposant n sont tous du degré ν, et nous avons vu que leur nombre est égal à $\frac{\varphi(n)}{\nu}$, φ ayant la signification habituelle.

Cela posé, désignons par μ le plus petit nombre, tel que $p^\mu - 1$ soit divisible par chacun des facteurs premiers qui divisent n, il est évident que ν sera un multiple de μ; car soit $\nu = \mu q + r$; les facteurs premiers de n divisent par hypothèse $p^{\mu q + r} - 1$ et $p^{\mu q} - 1$, qui est un multiple de $p^\mu - 1$; ils divisent, par suite, la différence $p^{\mu q + r} - p^{\mu q}$ ou $p^{\mu q}(p^r - 1)$. Mais cela est impossible, à

moins que r ne soit nul, puisque r est $<\mu$; donc on a

$$(1)\qquad \nu = q\mu.$$

Soit $\frac{p^\mu - 1}{d}$ le plus grand commun diviseur des nombres n et $p^\mu - 1$; si l'on fait

$$(2)\qquad n = \frac{p^\mu - 1}{d}\lambda,$$

λ et d seront premiers entre eux; on aura ensuite

$$(3)\qquad \frac{p^\nu - 1}{n} = \frac{d}{\lambda}\,\frac{p^{q\mu} - 1}{p^\mu - 1},$$

et, comme le premier membre de cette formule est un nombre entier, λ sera un diviseur de $\frac{p^{q\mu} - 1}{p^\mu - 1}$. En élevant à la puissance q l'identité

$$p^\mu = 1 + (p^\mu - 1),$$

il vient

$$(4)\qquad \left\{\begin{aligned} \frac{p^{q\mu} - 1}{p^\mu - 1} &= \frac{q}{1} + \frac{q(q-1)}{1.2}(p^\mu - 1) + \ldots \\ &+ \frac{q(q-1)\ldots(q-k+1)}{1.2\ldots k}(p^\mu - 1)^{k-1} + \ldots, \end{aligned}\right.$$

expression qui doit être divisible par λ.

Désignons par θ un facteur premier de λ, et soit θ^α la plus haute puissance de θ contenue dans λ. Comme θ est un diviseur de n et, par suite, de $p^\mu - 1$, on voit, par la formule (4), qu'il est aussi un diviseur de q; mais je dis en outre que, si θ n'est pas égal à 2, chacun des termes de l'expression (4) à partir du deuxième renferme une puissance plus élevée de θ que le premier terme. En effet, le rapport du terme général au premier terme peut être

mis sous la forme d'un produit de trois facteurs, savoir

$$(5)\qquad \frac{(q-1)(q-2)\ldots(q-k+1)}{1.2\ldots(k-1)}\times\left(\frac{p^\mu-1}{\theta}\right)^{k-1}\times\frac{\theta^{k-1}}{k};$$

les deux premiers facteurs sont des nombres entiers; quant au troisième facteur, il est supérieur à

$$1+\frac{(k-1)(\theta-1)}{k} \quad \text{ou à} \quad 1+\frac{(k-1)(\theta-2)}{k},$$

par suite, supérieur à 1, quand θ est >2, puisque k est au moins égal à 2; la fraction irréductible égale à $\frac{\theta^{k-1}}{k}$ renferme donc le facteur θ à son numérateur. Le premier membre de la formule (4) étant divisible par θ^α, par hypothèse, il faut, d'après ce qui précède, que q soit divisible par θ^α.

Si donc λ est un nombre impair, q sera divisible par λ. Réciproquement, si q est divisible par λ, l'expression (4) l'est évidemment elle-même, et en conséquence le premier membre de la formule (3) est un nombre entier. On voit alors que ν étant le plus petit nombre tel, que $p^\nu-1$ soit divisible par n, on doit avoir $q=\lambda$ et, par suite,

$$(6)\qquad \nu=\lambda\mu.$$

Examinons s'il y a lieu de modifier cette conclusion quand λ est pair. D'abord si λ est double d'un impair, l'expression (4) doit être divisible par 2, ce qui exige que q le soit aussi; donc, pour que l'expression (3) soit un nombre entier, il est encore nécessaire et suffisant que q soit un multiple de λ, et la formule (6) subsiste.

Supposons donc que λ soit divisible par une puissance de 2 supérieure à la première. Quand on fait $\theta=2$, dans l'expression (5), le troisième facteur devient $\frac{2^{k-1}}{k}$; il n'est jamais inférieur à 1, car k est au moins égal à 2, mais il

se réduit à 1 pour $k = 2$, et alors il peut arriver que les deux premiers termes de l'expression (4) renferment le facteur 2 à la même puissance. Toutefois ce cas ne se présentera pas si $p^\mu - 1$ est divisible par 4, c'est-à-dire si p est de la forme $4m + 1$, ou si, p étant de la forme $4m - 1$, μ est un nombre pair. Dans ces deux cas, la présence du facteur 2 dans λ n'exige aucune modification, et la formule (6) subsiste.

Mais il n'en est plus ainsi, dans le cas qu'il nous reste à examiner, savoir celui où p est de la forme $4m - 1$ et où μ est un nombre impair, λ étant divisible par une puissance de 2 supérieure à la première; il importe d'examiner ce cas avec attention. Dans l'hypothèse où nous nous plaçons, on a

$$p = 2^i . t - 1, \quad \lambda = 2^j . s,$$

t et s étant des nombres impairs et les exposants i, j étant égaux ou supérieurs à 2. Comme μ est impair, la première de ces formules donnera

$$p^\mu = 2^i \theta - 1,$$

θ étant un nombre impair; en outre, l'exposant q devant être pair, comme on l'a vu plus haut, on aura, en élevant la précédente formule à la puissance q,

$$(7)\left\{\begin{aligned} \frac{p^{\mu q} - 1}{p^\mu - 1} = \frac{2^{i-1}\theta}{2^{i-1}\theta - 1}\Bigg[& -\frac{q}{1} + \frac{q(q-1)}{1.2} 2^i\theta - \ldots \\ & \pm \frac{q\ldots(q-k+1)}{1.2\ldots k} 2^{i(k-1)}\theta^{k-1} \mp \ldots \Bigg]; \end{aligned}\right.$$

le rapport du terme général entre parenthèses au premier terme est

$$\frac{(q-1)\ldots(q-k+1)}{1.2\ldots(k-1)}\theta^{k-1} \times \frac{2^{i(k-1)}}{k};$$

i étant au moins 2, si l'on prend $k > 1$, le dernier facteur

de cette expression sera supérieur à 1, et la fraction irréductible qui lui est égale aura un numérateur pair; d'ailleurs les autres facteurs sont entiers, donc le premier des termes entre crochets, dans la formule (7), renferme le facteur 2 à une puissance moins élevée que les termes suivants. Alors si l'on désigne par ω le plus petit nombre de facteurs 2 qu'il faille introduire dans q pour que l'expression (3) soit entière, on aura

$$\omega = 1 \quad \text{ou} \quad \omega = j - i + 1,$$

savoir $\omega = 1$, si l'on a

$$j < \text{ou} = i,$$

car il suffit alors que q soit pair; et $\omega = j - i + 1$, si l'on a

$$j > i.$$

D'ailleurs, dans l'un et l'autre cas, q ne doit contenir que les seuls facteurs premiers impairs de λ; donc on a

$$q = \frac{\lambda}{2^{j-1}} \quad \text{ou} \quad q = \frac{\lambda}{2^{i-1}},$$

et par suite

$$\nu = \frac{\lambda\mu}{2^{j-1}}, \tag{8}$$

ou

$$\nu = \frac{\lambda\mu}{2^{i-1}}. \tag{9}$$

La formule (8) a lieu dans le cas de $j < i$, et la formule (9) dans le cas de $j > i$; les deux formules coïncident quand $j = i$.

356. Nous allons développer actuellement les conséquences de l'analyse précédente. Considérons d'abord le cas où la formule (6) a lieu, et désignons par N le nombre des fonctions entières irréductibles du degré ν

qui appartiennent à l'exposant n, on aura (n° 352)

$$N = \frac{\varphi(n)}{\nu} = \frac{\varphi(n)}{\lambda\mu},$$

ou, à cause de la formule (2),

$$N = \frac{1}{\mu}\,\frac{p^\mu - 1}{d}\,\frac{\varphi(n)}{n}.$$

Soit n' un nombre contenant tous les facteurs premiers de n avec des exposants quelconques, mais n'en contenant pas d'autres, on aura

$$\frac{\varphi(n')}{n'} = \frac{\varphi(n)}{n},$$

et puisque $\frac{p^\mu - 1}{d}$ est le plus grand commun diviseur de n et de $p^\mu - 1$, on peut prendre

$$n' = \frac{p^\mu - 1}{d}.$$

Remplaçant donc n par cette valeur n', l'expression de N devient

$$(10) \qquad N = \frac{1}{\mu}\,\varphi\left(\frac{p^\mu - 1}{d}\right),$$

d'où il résulte que N représente aussi le nombre des fonctions irréductibles de degré μ qui appartiennent à l'exposant $\frac{p^\mu - 1}{d}$.

Posons, pour abréger,

$$\frac{p^\mu - 1}{d} = \delta, \quad \text{d'où} \quad n = \delta\lambda,$$

et décomposons $x^\delta - 1$ en facteurs irréductibles suivant le module p; soit

$$(11) \qquad x^\delta - 1 = F(x)\,F_1(x)\,F_2(x)\ldots + p\chi(x).$$

μ est le plus petit nombre tel, que $x^{p^\mu}-1$ soit divisible par $x^\delta-1$ suivant le module p; car, s'il en était autrement et que δ divisât $p^{\mu'}-1$, μ' étant $<\mu$, le nombre $p^{\mu'}-1$ renfermerait tous les facteurs premiers de n, ce qui est contre l'hypothèse. Cette remarque nous confirme ce fait qui résulte d'ailleurs de notre analyse, savoir, que le degré de chaque facteur irréductible de la formule (11) est égal à μ ou à un diviseur de μ.

Remplaçons maintenant x par x^λ dans la formule (11), il viendra

$$(12)\qquad x^n-1=F(x^\lambda)F_1(x^\lambda)F_2(x^\lambda)+\ldots+p\chi(x^\lambda).$$

Soient

$$(13)\qquad F(x),\ F_1(x),\ \ldots,\ F_{N-1}(x)$$

les N facteurs du degré μ de la formule (11), il est évident que, dans la formule (12), les facteurs du degré $\lambda\mu=\nu$ seront

$$(14)\qquad F(x^\lambda),\ F_1(x^\lambda),\ \ldots,\ F_{N-1}(x^\lambda).$$

Or il y a N fonctions irréductibles du degré ν, lesquelles divisent x^n-1 suivant le module p; donc ces fonctions ne sont autre chose que les polynômes (14), ce qui donne le théorème suivant :

Théorème I. — *Si l'on a formé les* N *fonctions entières irréductibles de degré* μ *suivant le module* p, *qui appartiennent à l'exposant* $\frac{p^\mu-1}{d}$, *puis que l'on y remplace* x *par* x^λ, λ *étant un nombre premier avec* d *et qui ne renferme aucun facteur premier différent de ceux par lesquels* $p^\mu-1$ *est divisible, on obtiendra les* N *fonctions irréductibles du degré* $\lambda\mu$, *qui appartiennent à l'exposant* $\lambda\frac{p^\mu-1}{d}$. *Il faut cependant excepter le cas*

où, p étant de la forme $4i-1$, μ est un nombre impair et λ un nombre divisible par 4.

357. Considérons maintenant ce cas d'exception, dans lequel p est de la forme $4m-1$, μ un nombre impair et λ un nombre divisible par 4. Alors l'une des formules (8) et (9) a lieu, et si l'on désigne encore par N le nombre des fonctions entières irréductibles du degré ν qui appartiennent à l'exposant n, on aura

$$N = \frac{\varphi(n)}{\nu} = 2^{k-1}\frac{\varphi(n)}{\lambda\mu},$$

en nommant k le plus petit des deux nombres i et j; on peut écrire aussi, à cause de la formule (2),

$$N = 2^{k-1}\frac{1}{\mu}\frac{p^{\mu}-1}{d}\frac{\varphi(n)}{n}.$$

Comme tous les facteurs premiers de l'un des nombres n et $\frac{p^{\mu}-1}{d}$ appartiennent aussi à l'autre, on peut encore remplacer ici

$$\frac{p^{\mu}-1}{d}\frac{\varphi(n)}{n}$$

par $\varphi\left(\frac{p^{\mu}-1}{d}\right)$, et l'on a

$$N = 2^{k-1}\frac{1}{\mu}\varphi\left(\frac{p^{\mu}-1}{d}\right).$$

$\frac{N}{2^{k-1}}$ est donc le nombre des fonctions irréductibles de degré μ qui appartient à l'exposant $\frac{p^{\mu}-1}{d} = \delta$.

Nous conservons la formule (11), qui donne la décomposition du binôme $x^{\delta}-1$ en facteurs irréductibles, ainsi que la formule (12) qu'on en déduit en remplaçant x

par x^λ. Ceux des facteurs $F(x)$, $F_1(x)$, ... qui appartiennent à un exposant inférieur à δ donneront, dans la formule (12), des facteurs correspondants dont les diviseurs irréductibles appartiendront à un exposant moindre que n. Donc les facteurs irréductibles de $x^n - 1$ qui appartiennent à l'exposant $\nu = \frac{\lambda\mu}{2^{k-1}}$ sont nécessairement des diviseurs de l'un des $\frac{N}{2^{k-1}}$ polynômes

$$F(x^\lambda),\quad F_1(x^\lambda),\quad F_2(x^\lambda),\ \ldots,$$

qui répondent aux $\frac{N}{2^{k-1}}$ facteurs

$$F(x),\quad F_1(x),\quad F_2(x),\ \ldots,$$

relatifs à l'exposant δ. Les polynômes dont il s'agit sont du degré $\lambda\mu$, leur nombre est $\frac{N}{2^{k-1}}$, et le nombre des fonctions irréductibles du degré $\frac{\lambda\mu}{2^{k-1}}$ est N; donc chacun de nos polynômes est le produit de 2^{k-1} facteurs irréductibles du degré $\frac{\lambda\mu}{2^{k-1}}$. De là résulte la proposition suivante :

Théorème II. — *Soient p un nombre premier de la forme $2^i t - 1$, où i n'est pas inférieur à 2 et où t est un nombre impair; μ un nombre impair; $\frac{p^\mu - 1}{d}$ un diviseur de $p^\mu - 1$; λ un nombre de la forme $2^j s$, où j n'est pas inférieur à 2 et où s est un nombre impair; enfin k le plus petit des nombres i et j.*

Si l'on a formé les $\frac{N}{2^{k-1}}$ fonctions entières irréductibles de degré μ suivant le module q qui appartiennent à

l'exposant $\frac{p^\mu - 1}{d}$, *puis qu'on y remplace* x *par* x^λ, *le nombre* λ, *de la forme indiquée, étant premier avec* d *et ne renfermant que les seuls facteurs premiers qui figurent dans* $p^\mu - 1$, *on obtiendra* $\frac{N}{2^{k-1}}$ *fonctions du degré* $\lambda\mu$, *et chacune d'elles sera décomposable en* 2^{k-1} *facteurs irréductibles, ce qui donnera en tout* N *polynômes irréductibles du degré* $\frac{\lambda\mu}{2^{k-1}}$.

358. Désignons par g une racine primitive du nombre premier p; les fonctions du premier degré qui appartiennent à l'exposant $\frac{p-1}{d}$ seront évidemment $x - g^{\alpha d}$, α étant un nombre premier avec $\frac{p-1}{d}$. Si donc on représente ces fonctions par $x - g^e$, d sera le plus grand commun diviseur des nombres e et $p-1$. D'après cela, si l'on suppose $\mu = 1$, dans les énoncés des théorèmes I et II, on obtient cette proposition nouvelle, qui a une assez grande importance, savoir :

Théorème III. — *Soient* g *une racine primitive du nombre premier* p; λ *un nombre entier qui ne renferme aucun facteur premier différent de ceux qui divisent* $p-1$; e *un nombre entier premier avec* λ; d *le plus grand commun diviseur des nombres* e *et* $p-1$.

1° *Si* p *est de la forme* $4q+1$, *ou si,* p *étant de la forme* $4q-1$, *le nombre* λ *est impair ou double d'un impair, la fonction binôme* $x^\lambda - g^e$ *est irréductible suivant le module* p *et elle appartient à l'exposant* $\lambda\frac{p-1}{d}$.

2° *Si* p *et* λ *sont respectivement des formes* $p = 2^i t - 1$, $\lambda = 2^j s$, i *et* j *étant au moins égaux à* 2,

et t, s étant des nombres impairs; si, en outre, on désigne par k le plus petit des nombres i, j, la fonction binôme $x^\lambda - g^e$ est réductible suivant le module p, et elle se décompose en 2^{k-1} facteurs irréductibles du degré $\frac{\lambda}{2^{k-1}}$ qui, tous, appartiennent à l'exposant $\lambda\,\frac{p-1}{d}$.

Ce théorème nous fait connaître, sans aucune exception, toutes les fonctions binômes irréductibles suivant le module premier p. En effet, la fonction $x^\lambda - g^e \pmod{p}$ ne saurait être irréductible si λ et e ont un diviseur commun. En outre, si λ contient un facteur premier θ qui ne divise pas $p-1$, la congruence $x^\theta - g^e \equiv 0 \pmod{p}$ aura une racine et par suite $x^\theta - g^e$ admettra suivant le module p un diviseur de la forme $x-\alpha$; il s'ensuit que $x^{\frac{\lambda}{\theta}} - x$ sera pareillement un diviseur de $x^\lambda - g^e$.

359. Lorsque p est un nombre de la forme $2^i t - 1$ où i est au moins égal à 2 et où t est un nombre impair, il n'existe de fonctions binômes irréductibles de degré λ, ainsi qu'on vient de le voir, que dans le cas où λ est impair ou double d'un impair. Mais, quel que soit le nombre pair λ, pourvu qu'il ne renferme que les facteurs premiers par lesquels $p-1$ est divisible, on peut former facilement des fonctions trinômes de degré λ irréductibles suivant le module p.

En effet, le nombre p étant, par hypothèse, de la forme

$$p = 2^i t - 1,$$

et t étant impair, posons

$$\nu = 2^{i-1}\lambda,$$

le nombre ν sera divisible par 2^i, car λ est pair. Ensuite, si g désigne une racine primitive de p et que e soit un

nombre premier avec λ, la fonction

$$x^\nu - g^e$$

sera, d'après le théorème III (n° 358), décomposable en 2^{i-1} facteurs irréductibles du degré λ. Pour obtenir ces facteurs, remarquons d'abord que 2^i et $p-1$ ont 2 pour plus grand commun diviseur et que e et $\frac{p-1}{2}$ sont impairs; il en résulte que l'on pourra toujours trouver deux entiers θ et ζ tels, que l'on ait

$$2^i\theta - (p-1)\zeta = e + \frac{p-1}{2};$$

alors, g étant racine primitive de p, on aura

$$g^{2^i\theta} \equiv -g^e \pmod{p},$$

et la fonction que nous considérons sera

$$x^\nu - g^e \equiv x^{2^{i-1}\lambda} + g^{2^i\theta} \pmod{p}.$$

Cela posé, désignons par u et v deux variables; les deux fonctions

$$u^{\frac{p+1}{2}} + v^{\frac{p+1}{2}}, \quad u^{\frac{p-1}{2}} + v^{\frac{p-1}{2}}$$

seront divisibles algébriquement, la première par $u^{2^{i-1}} + v^{2^{i-1}}$, la seconde par $u+v$, car t et $\frac{p-1}{2}$ sont des nombres impairs; le produit de ces fonctions peut donc être mis sous la forme

$$(u+v)\left(u^{2^{i-1}} + v^{2^{i-1}}\right) f(u, v),$$

f étant un polynôme à coefficients entiers Mais si l'on effectue la multiplication des deux mêmes fonctions, on trouve le résultat

$$(u^p + v^p) + (u+v)(uv)^{\frac{p-1}{2}};$$

nous savons d'ailleurs que

$$(u^p + v^p) = (u+v)^p + p\chi(u, v);$$

et il est évident que $\chi(u, v)$ est divisible par $u+v$, en sorte qu'on peut écrire

$$(u^p + v^p) = (u+v)^p - p(u+v)f_1(u, v),$$

f_1 étant un polynôme à coefficients entiers. En égalant entre elles les deux expressions du produit que nous considérons, après avoir supprimé le facteur $u+v$, on obtient l'identité suivante :

$$(1)\quad (u+v)^{p-1} + (uv)^{\frac{p-1}{2}} = \left(u^{2^{i-1}} + v^{2^{i-1}}\right) f(u, v) + pf_1(u, v),$$

où f et f_1 sont évidemment des polynômes à coefficients entiers, fonctions symétriques des variables u et v.

Remplaçons maintenant u et v par les deux racines de l'équation

$$X^2 - \xi X - 1 = 0,$$

où ξ désigne une nouvelle variable; toutes les fonctions symétriques entières de u et v, à coefficients entiers, deviendront des fonctions entières de ξ, dans lesquelles les coefficients seront encore entiers; la formule (1) donnera donc

$$(2)\qquad \xi^{p-1} - 1 = E(\xi)\varphi(\xi) + p\chi(\xi),$$

en posant

$$E(\xi) = u^{2^{i-1}} + v^{2^{i-1}},$$

ou

$$(3)\quad E(\xi) = \left[\frac{\xi}{2} + \sqrt{\frac{\xi^2}{4} + 1}\right]^{2^{i-1}} + \left[\frac{\xi}{2} - \sqrt{\frac{\xi^2}{4} + 1}\right]^{2^{i-1}},$$

et en désignant par $\varphi(\xi)$, $\chi(\xi)$ des polynômes à coefficients entiers.

Maintenant, comme le polynôme $E(\xi)$ est un diviseur de

$$\xi^{p-1} - 1 - p\chi(\xi),$$

la congruence

$$(4) \qquad E(\xi) \equiv 0 \pmod{p},$$

qui est du degré 2^{i-1}, aura 2^{i-1} racines, et en désignant ces racines par

$$\xi_1,\ \xi_2,\ \ldots,\ \xi_{2^{i-1}},$$

on aura

$$(5) \qquad E(\xi) = (\xi - \xi_1)(\xi - \xi_2)\ldots(\xi - \xi_{2^{i-1}}) + p\varpi(\xi),$$

$\varpi(\xi)$ étant un polynôme à coefficients entiers.

Les formules (3) et (5) donnent pour $E(\xi)$ des valeurs qui doivent être identiques ; si on les égale entre elles, et qu'on pose

$$\xi = \frac{x^{\frac{\lambda}{2}}}{g^\theta} - \frac{g^\theta}{x^{\frac{\lambda}{2}}}, \quad \sqrt{\xi^2 + 4} = \frac{x^{\frac{\lambda}{2}}}{g^\theta} + \frac{g^\theta}{x^{\frac{\lambda}{2}}},$$

il viendra, après avoir chassé les dénominateurs,

$$x^{2^{i-1}\lambda} + g^{2^i\theta} = \prod\left(x^\lambda - \xi g^\theta x^{\frac{\lambda}{2}} - g^{2\theta}\right) + p\Phi(x);$$

$\Phi(x)$ désigne un polynôme à coefficients entiers, et le signe $\prod$ exprime le produit des facteurs que représente l'expression

$$x^\lambda - \xi g^\theta x^{\frac{\lambda}{2}} - g^{2\theta},$$

quand on prend pour ξ chacune des racines de la congruence (4). Les facteurs dont il s'agit sont précisément les fonctions irréductibles que nous voulions trouver.

Sur une fonction irréductible du degré p, suivant le module p.

360. La méthode que nous avons exposée au n° **351** pour former les fonctions irréductibles n'est guère susceptible d'être appliquée ; aussi doit-on attacher quelque importance aux théorèmes qui précèdent et qui permettent de former directement une fonction irréductible de degré λ, lorsque le nombre λ ne renferme que les facteurs premiers du module diminué de l'unité ; on verra effectivement plus loin que la connaissance d'une fonction irréductible d'un degré quelconque, suivant un module premier, suffit pour qu'on puisse former directement toutes les autres fonctions irréductibles du même degré.

Je présenterai encore ici une proposition qui fait connaître une fonction irréductible du degré premier p, suivant le module p.

Théorème. — *Si le nombre g n'est pas divisible par le nombre premier p, la fonction $x^p - x - g$ est irréductible suivant le module p.*

En effet, soit $F(x)$ un facteur irréductible, suivant le module p, de la fonction dont il s'agit. On aura

$$x^p - x - g \equiv F(x)\varphi(x) \pmod{p},$$

$\varphi(x)$ étant un polynôme à coefficients entiers. On tire de là

$$x^p \equiv x + g + F(x)\varphi(x) \pmod{p},$$

et, en élevant les deux membres à la puissance p^{m-1},

$$x^{p^m} \equiv x^{p^{m-1}} + g + F(x)\varphi(x) \pmod{p},$$

$\varphi(x)$ désignant encore ici un polynôme à coefficients entiers.

Faisons successivement $m = 1, 2, 3, \ldots$, il viendra

$$\left.\begin{array}{l} x^p \equiv x \quad + g + F(x)\varphi(x) \\ x^{p^2} \equiv x^p + g + F(x)\varphi(x) \equiv x + 2g + F(x)\varphi(x) \\ x^{p^3} \equiv x^{p^2} + g + F(x)\varphi(x) \equiv x + 3g + F(x)\varphi(x) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array}\right\} \pmod{p},$$

et l'on aura, quel que soit m,

$$x^{p^m} \equiv x + mg + F(x)\varphi(x) \pmod{p}.$$

Supposons maintenant que m désigne le degré de $F(x)$; alors, $F(x)$ divisant $x^{p^m} - x$, la formule précédente exige que l'on ait

$$mg \equiv 0 \quad \text{ou} \quad m \equiv 0 \pmod{p};$$

m étant ainsi un multiple de p, on a $m = p$; par suite $F(x)$ ne peut être que la fonction $x^p - x - g$ elle-même.

Classification des fonctions réduites suivant un module premier et suivant une fonction irréductible.

361. Soit $F(x)$ une fonction entière irréductible suivant le module premier p; si l'on pose

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{\nu-1} x^{\nu-1},$$

$a_0, a_1, \ldots, a_{\nu-1}$ étant des entiers compris entre 0 et $p-1$, ou entre $-\frac{p-1}{2}$ et $+\frac{p-1}{2}$, $f(x)$ sera l'expression générale des fonctions réduites suivant le module p et suivant la fonction irréductible $F(x)$. Le nombre total de ces fonctions réduites est p^ν et nous avons vu que chacune d'elles satisfait à la condition

$$[f(x)]^{p^\nu} - f(x) \equiv F(x)\psi(x) \pmod{p},$$

qui exprime que la fonction

$$[f(x)]^{p^\nu} - f(x)$$

est divisible par $F(x)$ suivant le module p.

Nous nous proposons d'établir ici à l'égard des fonctions $f(x)$ une classification de tout point semblable à celle que nous avons faite pour les nombres entiers dans le Chapitre précédent. L'analyse que nous allons développer ne suppose pas le théorème que nous venons de rappeler; celui-ci, au contraire, se présentera comme une conséquence de cette analyse.

Dans ce qui va suivre je ferai usage d'une notation particulière qu'il convient, je crois, d'introduire dans la théorie qui nous occupe. Puisque nous écrivons $A \equiv B$ (mod. p) pour exprimer que la différence des nombres A et B est divisible par p, il semble naturel d'admettre la notation

$$\mathfrak{F}(x) \equiv f(x) \quad [\text{mod. } p,\ F(x)]$$

pour exprimer que la différence des deux fonctions entières $\mathfrak{F}(x)$, $f(x)$ est divisible, suivant le module p, par la fonction irréductible $F(x)$. Celle-ci prendra alors le nom de *fonction modulaire*, et je dirai que $\mathfrak{F}(x)$ et $f(x)$ sont *congrues suivant le module p et suivant la fonction modulaire* $F(x)$. Enfin, pour abréger le langage, je donnerai le nom de *résidus minima* aux fonctions réduites suivant le module et suivant la fonction modulaire.

362. Cela posé, soit X l'une quelconque des $p^\nu - 1$ valeurs de $f(x)$ autres que zéro; nous ferons, dans ce qui va suivre, abstraction de la valeur zéro. Les résidus minima des termes de la suite

$$1,\ X,\ X^2,\ X^3,\ \ldots$$

seront aussi des valeurs de $f(x)$. Mais, parce que $f(x)$

n'a que $p^\nu - 1$ valeurs distinctes, il faut que quelques-unes de ces valeurs se trouvent reproduites une infinité de fois dans la série des puissances de X. Supposons que l'on ait

$$X^{n+n'} \equiv X^{n'} \quad [\text{mod. } p,\ F(x)],$$

ou

$$X^{n'}(X^n - 1) \equiv 0 \quad [\text{mod. } p,\ F(x)].$$

Comme $X^{n'}$ ne peut être divisible par $F(x)$, suivant le module p, il faut que l'on ait

$$X^n \equiv 1 \quad [\text{mod. } p,\ F(x)],$$

et, par suite,

$$X^{2n} \equiv 1, \quad X^{3n} \equiv 1, \quad \ldots \quad [\text{mod. } p,\ F(x)].$$

Il y a donc une infinité de puissances de X congrues à l'unité. Soit n le plus petit nombre tel, que l'on ait

$$X^n \equiv 1 \quad [\text{mod. } p,\ F(x)],$$

on aura ces n valeurs de $f(x)$ dont les résidus minima seront distincts, savoir

(1) $$1,\ X,\ X^2,\ X^3,\ \ldots,\ X^{n-1}.$$

Si l'on a $p^\nu - 1 = n$, la suite (1), ou celle de ses résidus minima, comprendra toutes les valeurs de $f(x)$.

Si l'on a $p^\nu - 1 > n$, soit X_1 l'une des valeurs de $f(x)$ qui ne sont pas comprises parmi les résidus minima de la suite (1); en multipliant les fonctions (1) par X_1, on obtient les nouvelles fonctions

(2) $$X_1,\ XX_1,\ X^2X_1,\ \ldots,\ X^{n-1}X_1,$$

dont les résidus minima sont distincts; car soient n' et n'' deux nombres inférieurs à n; si l'on avait

$$X^{n'}X_1 - X^{n''}X_1 \equiv 0 \quad [\text{mod. } p,\ F(x)],$$

comme X_1 ne peut être divisible par $F(x)$, suivant le

module p, on aurait

$$X^{n'} - X^{n''} \equiv 0 \quad [\text{mod. } p, \ F(x)],$$

ce qui est contre l'hypothèse. En outre, les quantités (2) sont distinctes de (1); car si l'on avait, par exemple,

$$X^{n'} X_1 \equiv X^{n''} \quad [\text{mod. } p, \ F(x)],$$

on aurait, en multipliant par $X^{n-n'}$,

$$X^n X_1 \equiv X^{n-n'+n''} \quad \text{ou} \quad X_1 = X^{n-n'+n''} \quad [\text{mod. } p, \ F(x)],$$

ce qui est encore contraire à l'hypothèse.

Il résulte de là que $p^\nu - 1$ est égal ou supérieur à $2n$. Si $p^\nu - 1$ est $> 2n$, soit X_2 une valeur de $f(x)$ non comprise parmi les résidus minima des suites (1) et (2). En multipliant les fonctions (1) par X_2, on obtient les nouvelles fonctions

$$(3) \qquad X_2, \ XX_2, \ X^2X_2, \ \ldots, \ X^{n-1}X_2.$$

Le raisonnement que nous venons de faire prouve que les résidus minima de ces fonctions (3) sont différents entre eux et distincts des résidus fournis par la suite (1); il est aisé de voir qu'ils sont aussi distincts des résidus de la suite (2); car si l'on avait, par exemple,

$$X^{n'} X_2 \equiv X^{n''} X_1 \quad [\text{mod. } p, \ F(x)],$$

en multipliant par $X^{n-n'}$, il viendrait

$$X^n X_2 \equiv X^{n-n'+n''} X_1 \quad \text{ou} \quad X_2 \equiv X^{n-n'+n''} X_1 \quad [\text{mod. } p, F(x)],$$

ce qui est contre l'hypothèse.

Il résulte de là que $p^\nu - 1$ est égal ou supérieur à $3n$. Et, en poursuivant ce raisonnement, on voit que $p^\nu - 1$ est nécessairement un multiple de n.

Si n est le plus petit nombre tel, que l'on ait

$$X^n \equiv 1 \quad [\text{mod. } p, \ F(x)],$$

je dirai que la fonction X *appartient à l'exposant n, suivant le module p et la fonction modulaire* F(x). Ce nombre n étant un diviseur de $p^\nu - 1$, la précédente congruence entraîne

$$X^{p^\nu - 1} - 1 \equiv 0 \quad [\text{mod. } p, \; F(x)],$$

ce qui fournit une nouvelle démonstration du théorème démontré au n° 346.

363. Théorème I. — *La fonction* F(x), *irréductible suivant le module p, étant du degré ν et n désignant un diviseur quelconque de $p^\nu - 1$, il y a autant de fonctions réduites qui appartiennent à l'exposant n, suivant le double module* [p, F(x)], *qu'il y a d'unités dans le nombre* $\varphi(n)$ *qui exprime la totalité des nombres premiers et non supérieurs à n.*

La démonstration de ce théorème est identique à celle dont nous avons fait usage au n° 306, en nous occupant de la classification des nombres entiers relativement à un module premier. Nous la reproduirons cependant, à cause de l'importance du sujet.

Supposons qu'il existe une fonction X_1 appartenant à l'exposant n; les résidus minima des fonctions

$$(1) \qquad 1, \; X_1, \; X_1^2, \; \ldots, \; X_1^{n-1}$$

seront distincts; d'ailleurs, si e désigne l'un quelconque des nombres

$$1, \; 2, \; 3, \; \ldots, \; (n-1),$$

la congruence

$$X_1^n \equiv 1 \quad [\text{mod. } p, \; F(x)]$$

entraînera

$$(2) \qquad X_1^{ne} \equiv 1 \quad \text{ou} \quad (X_1^e)^n \equiv 1 \quad [\text{mod. } p, \; F(x)],$$

d'où il résulte que, si l'on substitue chacune des n fonctions (1) à X dans la fonction

$$X^n - 1,$$

on obtiendra n résultats qui seront divisibles par $F(x)$ suivant le module p; donc, d'après la proposition du n° 345, il n'existe aucune fonction réduite autre que les résidus des fonctions (1) dont la puissance $n^{\text{ième}}$ soit divisible par $F(x)$ suivant le module p.

Désignons maintenant par m l'exposant auquel appartient X_1^e, c'est-à-dire le plus petit nombre tel, que l'on ait

$$(3) \qquad (X_1^e)^m = X_1^{me} \equiv 1 \quad [\text{mod. } p,\ F(x)].$$

La congruence (2) exige que n soit un multiple de m; inversement, comme X_1 appartient à l'exposant n, la congruence (3) exige que me soit un multiple de n, et, par suite, que m soit divisible par n, lorsque e est premier à n. Donc on a $m = n$, dans cette hypothèse; ainsi X_1^e appartient à l'exposant n lorsque e est premier à n. Mais, si n et e ont un diviseur commun $\theta > 1$, on aura

$$(X_1^e)^{\frac{n}{\theta}} = \left(X_1^{\frac{e}{\theta}}\right)^n \equiv 1 \quad [\text{mod. } p,\ F(x)];$$

et, par conséquent, X_1^e n'appartient pas à l'exposant n. Si donc il existe des fonctions réduites appartenant à l'exposant n, le nombre de ces fonctions est égal à $\varphi(n)$, $\varphi(n)$ indiquant, comme à l'ordinaire, combien il y a de nombres premiers et non supérieurs à n.

Cela posé, toute fonction réduite appartient à un exposant qui est l'un des diviseurs

$$d,\ d',\ d'',\ \ldots$$

de $p^\nu - 1$. Si donc on nomme $\psi(n)$ le nombre des fonc-

tions réduites qui appartiennent à l'exposant n, on aura

$$\psi(d)+\psi(d')+\psi(d'')+\ldots=p^\nu-1,$$

et, par suite,

$$\psi(d)+\psi(d')+\psi(d'')+\ldots=\varphi(d)+\varphi(d')+\varphi(d'')+\ldots.$$

Mais, d'après ce qu'on a vu plus haut, on a

$$\psi(n)=\varphi(n) \quad \text{ou} \quad \psi(n)=0;$$

le dernier cas ne saurait jamais avoir lieu, à cause de l'égalité qui précède; donc on a

$$\psi(n)=\varphi(n).$$

Corollaire. — *Il y a* $\varphi(p^\nu-1)$ *fonctions réduites qui appartiennent à l'exposant* $p^\nu-1$, *suivant le module* p *et la fonction modulaire* $F(x)$.

364. Théorème II. — *Si deux fonctions réduites* X_1, X_2 *appartiennent, relativement au module* p *et à la fonction modulaire* $F(x)$, *à des exposants* n_1, n_2 *premiers entre eux, le résidu minimum du produit* X_1X_2 *appartiendra à l'exposant* n_1n_2.

En effet, soit s un exposant tel, que

(1) $$(X_1X_2)^s=X_1^sX_2^s\equiv 1 \quad [\text{mod. } p,\ F(x)],$$

on aura, par l'élévation à la puissance n_1,

$$X_1^{sn_1}X_2^{sn_1}\equiv 1 \quad [\text{mod. } p,\ F(x)],$$

et, puisque X_1 appartient à l'exposant n_1, cette congruence se réduit à

(2) $$X_2^{sn_1}\equiv 1 \quad [\text{mod. } p,\ F(x)].$$

La congruence (2) montre que sn_1 est un multiple

de n_2; mais n_1 et n_2 sont premiers entre eux, donc s est divisible par n_2. D'ailleurs n_2 est l'un quelconque des nombres n_1, n_2, par suite s est divisible par n_1 et par n_2; il l'est donc également par le produit $n_1 n_2$.

Enfin la congruence (1) étant satisfaite quand on prend $s = n_1 n_2$, on voit que $n_1 n_2$ est effectivement l'exposant auquel appartient le produit $X_1 X_2$.

Corollaire I. — *Si les fonctions réduites* $X_1, X_2, \ldots, X_i$ *appartiennent, relativement au module* p *et à la fonction modulaire* $F(x)$, *à des exposants* $n_1, n_2, \ldots, n_i$ *qui soient premiers entre eux, deux à deux, le résidu minimum de la fonction* $X_1 X_2 \ldots X_i$ *appartiendra à l'exposant* $n_1 n_2 \ldots n_i$.

Corollaire II. — *Si le nombre* $p^\nu - 1$ *est égal à* $2^\rho q^\lambda r^\mu \ldots, q, r, \ldots$ *étant des nombres premiers impairs inégaux, et si* $X_0, X_1, X_2, \ldots$ *désignent des fonctions réduites appartenant respectivement aux exposants* 2^ρ, q^λ, r^μ, ..., *le produit* $X_0 X_1 X_2 \ldots$, *ou son résidu minimum, appartiendra à l'exposant* $p^\nu - 1$.

Des congruences suivant un module premier et suivant une fonction modulaire.

365. Soit $\mathfrak{F}(X)$ une fonction entière de la variable X, dans laquelle les coefficients des puissances de X soient des nombres entiers ou des fonctions entières de la variable x, prises suivant le module p et suivant la fonction irréductible $F(x)$ d'un degré quelconque ν. Je dirai que la valeur

$$X = f(x)$$

est une racine de la congruence

$$\mathfrak{F}(X) \equiv 0 \quad [\text{mod. } p,\ F(x)],$$

si, après la substitution de $f(x)$ à X, la fonction $\mathfrak{F}(X)$ est divisible par $F(x)$, suivant le module p.

Le corollaire du théorème démontré au n° 345 peut alors être énoncé comme il suit :

Une congruence du degré m, suivant un module premier et suivant une fonction irréductible, a au plus autant de racines qu'il y a d'unités dans son degré.

366. Théorème I. — *Soient* $F(x)$ *et* $\mathfrak{F}(x)$ *deux fonctions irréductibles suivant le module p, la première du degré* ν, *la deuxième d'un degré égal à* ν *ou à un diviseur de* ν. *La congruence*

$$\mathfrak{F}(X) \equiv 0 \quad [\text{mod. } p, \ F(x)]$$

a précisément autant de racines qu'il y a d'unités dans son degré.

En effet, le degré de $\mathfrak{F}(X)$ étant un diviseur de ν, on a

$$X^{p^\nu} - X = \mathfrak{F}(X)\,\mathfrak{F}_1(X) + p\chi(X),$$

$\mathfrak{F}_1(X)$ et $\chi(X)$ étant des polynômes à coefficients entiers. D'un autre côté, la congruence

$$X^{p^\nu} - X \equiv 0 \quad [\text{mod. } p, \ F(x)]$$

a pour racines les p^ν fonctions réduites de x, zéro compris; d'ailleurs chacune des racines de cette congruence appartient à l'une ou à l'autre des deux

$$\mathfrak{F}(X) \equiv 0, \quad \mathfrak{F}_1(X) \equiv 0 \quad [\text{mod. } p, \ F(x)],$$

et si l'une d'elles avait moins de racines qu'il n'y a d'unités dans son degré, il faudrait que l'autre en eût plus qu'il n'y a d'unités dans le sien, ce qui est impossible. Le théorème énoncé est donc établi.

367. THÉORÈME II. — *Si $\Phi(X)$ est un polynôme du degré m dont les coefficients soient des nombres entiers, et dans lequel le coefficient de X^m ne se réduise pas à zéro, suivant le module p, on pourra trouver une fonction irréductible $F(x)$ suivant le module p telle, que la congruence*

$$\Phi(X) \equiv 0 \quad [\text{mod. } p, \ F(x)]$$

ait m racines.

En effet, décomposons le polynôme $\Phi(X)$ en facteurs irréductibles suivant le module p; soit

$$\Phi(X) \equiv \Phi_1(X)\,\Phi_2(X)\,\Phi_3(X)\ldots \quad (\text{mod. } p),$$

et désignons par $n_1, n_2, n_3, \ldots$ les nombres inégaux par lesquels on peut exprimer les degrés des polynômes irréductibles $\Phi_1, \Phi_2, \ldots$. Chacun de ces facteurs divisera, suivant le module p, l'une des fonctions

$$X^{p^{n_1}} - X, \quad X^{p^{n_2}} - X, \quad X^{p^{n_3}} - X, \quad \ldots;$$

si donc ν désigne le plus petit nombre divisible à la fois par $n_1, n_2, \ldots$, les mêmes polynômes diviseront aussi

$$X^{p^\nu} - X.$$

Par conséquent, si l'on prend une fonction irréductible $F(x)$ de degré ν, chacune des congruences

$$\left.\begin{array}{l} \Phi_1(X) \equiv 0 \\ \Phi_2(X) \equiv 0 \\ \Phi_3(X) \equiv 0 \\ \ldots\ldots\ldots \end{array}\right\} [\text{mod. } p, \ F(x)]$$

aura (n° 366) autant de racines qu'il y a d'unités dans son degré, et il s'ensuit que la proposée aura elle-même autant de racines égales ou inégales qu'il y a d'unités dans son degré.

Propriétés des racines d'une congruence dont le premier membre est une fonction irréductible de degré égal au degré de la fonction modulaire ou égal à un sous-multiple de ce degré.

368. Théorème. — *Si* $F(x)$ *et* $\mathfrak{F}(x)$ *sont deux fonctions entières irréductibles suivant le module* p, *la première du degré* ν, *la seconde d'un degré* μ *égal à* ν *ou à un sous-multiple de* ν; *si en outre* X_1 *désigne l'une quelconque des racines de la congruence*

$$(1) \qquad \mathfrak{F}(X) \equiv 0 \quad [\text{mod. } p, \ F(x)],$$

les racines de cette congruence seront les résidus minima des puissances

$$(2) \qquad X_1, \ X_1^{p}, \ X_1^{p^2}, \ \ldots, \ X_1^{p^{\mu-1}}.$$

En effet, on a (n° 347)

$$\mathfrak{F}(X_1^{p^m}) \equiv [\mathfrak{F}(X_1)]^{p^m} \quad (\text{mod. } p),$$

et puisque X_1 satisfait à la congruence (1), on aura

$$\mathfrak{F}(X_1^{p^m}) \equiv 0 \quad [\text{mod. } p, \ F(x)];$$

donc chacune des puissances (2) ou son résidu minimum est racine de la proposée. Il reste à prouver que les résidus de ces puissances sont distincts. Si l'on avait

$$X_1^{p^{m+n}} \equiv X_1^{p^m} \quad [\text{mod. } p, \ F(x)],$$

il s'ensuivrait

$$X_1^{p^m}[X_1^{p^m(p^n-1)} - 1] \equiv 0 \quad [\text{mod. } p, \ F(x)],$$

puis

$$X_1^{p^m(p^n-1)} - 1 \equiv 0 \quad [\text{mod. } p, \ F(x)].$$

L'exposant auquel appartient X_1 est donc un diviseur

de $p^{n'}(p^n - 1)$ et, par suite, un diviseur de $p^n - 1$, car cet exposant ne renferme pas le facteur p; on a en conséquence

$$X^{p^n} - 1 \equiv 0 \quad [\text{mod. } p,\ F(x)].$$

Mais cela est impossible, puisque n est $< \mu$; donc les résidus des puissances (2) sont distincts.

COROLLAIRE. — *Si* $F(x)$ *désigne une fonction irréductible du degré* ν *suivant le module premier* p, *la congruence*

$$F(X) \equiv 0 \quad [\text{mod. } p,\ F(x)]$$

a pour racines les résidus minima des ν *puissances*

$$x,\ x^p,\ x^{p^2},\ \ldots,\ x^{p^{\nu-1}}.$$

Des racines primitives de la congruence
$$X^{p^\nu - 1} - 1 \equiv 0 \quad [\text{mod. } p,\ F(x)].$$

369. Quelle que soit la fonction entière $F(x)$ de degré ν, irréductible suivant le module premier p, parmi les $p^\nu - 1$ racines de la congruence

$$(1) \qquad X^{p^\nu - 1} - 1 \equiv 0 \quad [\text{mod. } p,\ F(x)],$$

il y en a $\varphi(p^\nu - 1)$ qui appartiennent (n° 363) à l'exposant $p^\nu - 1$; nous les nommerons *racines primitives*.

Si X désigne l'une quelconque des racines primitives, les racines de la précédente congruence seront les résidus minima des puissances

$$X,\ X^2,\ X^3,\ \ldots,\ X^{p^\nu - 1}.$$

Le nombre $p^\nu - 1$ étant décomposé en un produit $2^\rho q^\mu r^\lambda \ldots$ de facteurs premiers, pour avoir une racine primitive de la congruence (1), il suffira, d'après le co-

rollaire II du n° **364**, de former les congruences

$$(2)\quad X^{2^\rho}-1\equiv 0,\ X^{q^\mu}-1\equiv 0,\ X^{r^\lambda}-1\equiv 0\ldots\ [\text{mod.}\ p,\ F(x)],$$

et de chercher des racines de ces congruences qui appartiennent respectivement aux exposants 2^ρ, q^μ, r^λ, ... Ces dernières racines peuvent être nommées *primitives* à l'égard de celles des congruences (2) auxquelles elles se rapportent.

Si la fonction modulaire $F(x)$ est choisie parmi les fonctions irréductibles du degré ν qui appartiennent à l'exposant $p^\nu-1$, il est évident que les $p^\nu-1$ racines de la congruence (1) seront les résidus des puissances

$$x,\ x^2,\ x^3,\ \ldots,\ x^{p^\nu-2},\ x^{p^\nu-1},$$

car x est, dans ce cas, une racine primitive de la congruence.

370. Lorsque l'on connaît une fonction irréductible $F(x)$ de degré ν, relativement au module p, et qu'on a obtenu, au moyen de cette fonction, une racine primitive de la congruence

$$(1)\qquad X^{p^\nu-1}-1\equiv 0\quad [\text{mod.}\ p,\ F(x)],$$

on peut trouver facilement toutes les fonctions irréductibles dont le degré est égal à ν ou à un diviseur de ν. En d'autres termes, on peut effectuer la décomposition de la fonction

$$x^{p^\nu}-x\quad \text{ou}\quad X^{p^\nu}-X$$

en facteurs irréductibles suivant le module p.

En effet, soit X_1 une racine primitive de la congruence (1); toute puissance X_1^e sera racine d'une congruence telle que

$$(2)\qquad \mathfrak{F}(X)\equiv 0\quad [\text{mod.}\ p,\ F(x)],$$

$\mathfrak{F}(X)$ étant une fonction irréductible suivant le module p, dont le degré μ est égal à ν ou à un diviseur de ν. Alors les racines de la congruence (2) seront (n° 368)

$$(3) \qquad X_1^e,\ X_1^{ep},\ X_1^{ep^2},\ \ldots,\ X_1^{ep^{\mu-1}},$$

et, comme on doit avoir

$$(4) \qquad X_1^{ep^\mu} \equiv X_1^e \quad \text{ou} \quad X_1^{e(p^\mu-1)} \equiv 1 \quad [\text{mod}.\ p,\ F(x)],$$

l'exposant $e(p^\mu - 1)$ sera un multiple de $p^\nu - 1$. Posons

$$p^\nu - 1 = mn,$$

et supposons que m soit le plus grand commun diviseur des nombres e et $p^\nu - 1$; la condition pour que la congruence (4) ait lieu se réduira à celle de la divisibilité de $p^\mu - 1$ par n. Mais, pour que les fonctions (3) soient effectivement distinctes, il faut en outre que μ soit le plus petit nombre tel, que $p^\mu - 1$ soit divisible par n.

Le degré μ de la congruence (2) étant ainsi déterminé, on aura identiquement (n° 345)

$$\mathfrak{F}(X) \equiv (X - X_1^e)(X - X_1^{ep})\ldots(X - X_1^{ep^{\mu-1}}) \quad [\text{mod}.\ p,\ F(x)],$$

et, après avoir effectué le produit des binômes contenus dans le second membre de cette formule, on aura une expression de $\mathfrak{F}(X)$ de laquelle la variable x aura disparu.

On pourra former de cette manière toutes les fonctions irréductibles dans lesquelles la fonction $X^{p^\nu} - X$ peut être décomposée.

Si l'on désigne par k l'exposant auquel appartient X_1^e, on aura

$$X_1^{ke} \equiv 1 \quad [\text{mod}.\ p,\ F(x)],$$

d'où il résulte que ke est divisible par $p^\nu - 1 = mn$, et que, par suite, k est un multiple de n; mais comme la

congruence précédente est satisfaite par $k = n$, on voit que X_1^e appartient à l'exposant n.

Je dis en outre que la fonction irréductible $\mathfrak{F}(X)$ appartient à l'exposant n. En effet, désignons par $\mathfrak{F}_1(X)$ et $\Phi(X)$ le quotient et le reste de la division de $X^n - 1$ par $\mathfrak{F}(X)$ suivant le module p, on aura

$$X^n - 1 = \mathfrak{F}(X)\mathfrak{F}_1(X) + \Phi(X) + p\chi(X),$$

χ étant une fonction entière. Cela posé, les congruences

$$X^n - 1 \equiv 0, \quad \mathfrak{F}(X) \equiv 0 \quad [\text{mod.}\, p,\ F(x)]$$

admettent les μ racines qui forment la suite (3); donc ces racines appartiendront aussi à la congruence

$$\Phi(X) \equiv 0 \quad [\text{mod.}\, p,\ F(x)],$$

et comme celle-ci ne peut être d'un degré supérieur à $\mu - 1$, elle est nécessairement identique et l'on a

$$\Phi(X) \equiv 0 \quad (\text{mod.}\, p),$$

d'où

$$X^n - 1 = \mathfrak{F}(X)\mathfrak{F}_1(X) + p\chi(X),$$

ce qui exprime la proposition énoncée.

371. D'après ce que nous venons de voir, si l'on veut former toutes les fonctions irréductibles du degré ν qui appartiennent à l'exposant n, diviseur propre de $p^\nu - 1$, on posera

$$p^\nu - 1 = mn,$$

et l'on prendra ensuite pour e l'un quelconque des multiples de m premiers à n. L'expression générale des fonctions demandées sera

$$\mathfrak{F}(X) \equiv (X - X_1^e)(X - X_1^{ep}) \ldots (X - X_1^{ep^{\nu-1}}) \quad [\text{mod.}\, p,\ F(x)].$$

Si l'on veut avoir les fonctions irréductibles qui appartiennent à l'exposant $p^\nu - 1$ et auxquelles répondent les racines primitives, on fera $m = 1$, $n = p^\nu - 1$, en sorte qu'il suffira de prendre pour e, dans la formule précédente, tous les nombres premiers à $p^\nu - 1$ et à p.

Du point de vue sous lequel Galois a envisagé les congruences suivant un module premier et une fonction modulaire.

372. Dans la théorie des congruences ordinaires, on traite comme s'ils étaient nuls tous les nombres divisibles par le module. Et de même, dans l'analyse qui se rapporte aux congruences de la forme

$$\mathfrak{F}(X, x) \equiv 0 \quad [\text{mod. } p, F(x)],$$

on opère comme si les multiples de $F(x)$ s'évanouissaient. Or il y a ici une indéterminée x qu'on peut faire servir naturellement à l'évanouissement des multiples de $F(x)$; il suffit effectivement de convenir que cette indéterminée x est une *racine imaginaire* de la *congruence irréductible*

$$F(x) \equiv 0 \quad (\text{mod. } p).$$

Ainsi peuvent s'introduire dans l'analyse de nouvelles imaginaires dont l'emploi offre certains avantages, bien qu'il ne soit pas indispensable. Cette conception est entièrement due à Galois, qui l'a exposée succinctement dans le *Bulletin des Sciences mathématiques de Férussac* (t. XIII, p. 398) (¹).

(¹) L'article publié par Galois en 1830 dans le *Bulletin de Férussac* a été réimprimé ensuite avec ses autres Mémoires dans le tome XI du *Journal de Mathématiques pures et appliquées*.

La théorie que nous avons développée nous donne, au point de vue de Galois, les propositions suivantes :

Théorème I. — *Si i désigne une racine imaginaire de la congruence irréductible de degré ν,*

$$F(x) \equiv 0 \pmod{p}$$

une congruence non identique de degré m,

$$\varphi(x) \equiv 0 \pmod{p}$$

ne peut avoir plus de m racines distinctes de la forme

$$a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

où $a_0, a_1, \ldots, a_{\nu-1}$ *désignent des entiers inférieurs à p.*

Théorème II. — *La congruence*

$$x^{p^\nu} - x \equiv 0 \pmod{p}$$

admet toutes les p^ν *racines de la forme*

$$a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

i désignant une racine de la congruence irréductible

$$F(x) \equiv 0 \pmod{p},$$

de degré ν.

Théorème III. — *La congruence irréductible*

$$F(x) \equiv 0 \pmod{p}$$

de degré ν admet ν racines qui peuvent être représentées par

$$i, \; i^p, \; i^{p^2}, \; \ldots, \; i^{p^{\nu-1}}.$$

Théorème IV. — *Une congruence quelconque non identique a autant de racines égales ou inégales qu'il y a d'unités dans son degré; toutes ces racines sont des fonctions entières d'une même racine imaginaire d'une congruence irréductible.*

THÉORÈME V. — *La congruence*

$$x^{p^\nu - 1} - 1 \equiv 0 \pmod{p}$$

admet des racines primitives; chacune de celles-ci est racine d'une congruence irréductible de degré ν, *et ses puissances fournissent toutes les racines de la congruence proposée.*

THÉORÈME VI. — *Si l'on a* $p^\nu - 1 = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_m^{\alpha_m}$, $q_1, q_2, \ldots, q_m$ *étant des nombres premiers inégaux et* $\alpha_1, \alpha_2, \ldots, \alpha_m$ *des entiers quelconques, et que* r_1, $r_2, \ldots, r_m$ *désignent des racines primitives pour les congruences respectives,*

$$x^{q_1^{\alpha_1}} - 1 \equiv 0, \quad x^{q_2^{\alpha_2}} - 1 \equiv 0, \quad \ldots, \quad x^{q_m^{\alpha_m}} - 1 \equiv 0 \pmod{p},$$

le produit $r_1 r_2 \ldots r_m$ *sera une racine primitive de la congruence*

$$x^{p^\nu - 1} - 1 \equiv 0 \pmod{p}.$$

Application de la théorie précédente au cas du module 7.

373. Il ne sera pas inutile d'examiner quelques-uns des cas d'un module particulier. Je choisirai à cet effet le module 7, qui a 3 pour racine primitive, et je prendrai les résidus suivant ce module, entre les limites -3 et $+3$.

De la congruence $x^{7^2-1} - 1 \equiv 0 \pmod{7}$. — Le théorème du nº 358 nous donne immédiatement les trois fonctions irréductibles du deuxième degré

$$x^2 + 1, \quad x^2 + 2, \quad x^2 - 3.$$

Nous plaçant ici au point de vue de Galois, cherchons

une racine primitive de la congruence

$$(1) \qquad x^{7^2-1}-1\equiv 0 \quad \text{ou} \quad x^{48}-1\equiv 0,$$

en partant de la racine i de la congruence irréductible

$$(2) \qquad x^2+1\equiv 0 \pmod{7}.$$

A cet effet, comme $48 = 2^4\times 3$, il nous faut connaître une racine primitive des deux

$$(3) \qquad x^3-1\equiv 0, \quad x^{16}-1\equiv 0 \pmod{7}.$$

La première de ces congruences a 2 pour racine primitive, et les racines primitives de la deuxième appartiennent à

$$(4) \qquad x^8+1\equiv 0 \pmod{7},$$

laquelle, à cause de $i^2\equiv -1$, se décompose en deux autres, savoir :

$$x^4-i\equiv 0, \quad x^4+i\equiv 0 \pmod{7}.$$

Considérons la première

$$x^4-i\equiv 0 \pmod{7},$$

et posons

$$x = a_0 + a_1 i,$$

il viendra

$$a_0^4 - 3a_0^3a_1 i - a_0^2a_1^2 i^2 - 3a_0a_1^3 i^3 + a_1^4 i^4 \equiv i \pmod{7},$$

et, en réduisant à l'aide de $i^2\equiv -1$,

$$(a_0^4 + a_0^2a_1^2 + a_1^4) + (-3a_0^3a_1 + 3a_0a_1^3 - 1)i \equiv 0 \pmod{7},$$

d'où

$$a_0^4 + a_0^2a_1^2 + a_1^4\equiv 0, \quad -3a_0^3a_1 + 3a_0a_1^3 - 1\equiv 0 \pmod{7}.$$

On satisfait à ces congruences en posant

$$a_0 = 2, \quad a_1 = -3;$$

donc la deuxième des congruences (3) a la racine primi-

tive $2 - 3i$; par suite la proposée a la racine primitive

(5) $$x = 2 \times (2 - 3i) \equiv -3 + i \pmod{7}.$$

En élevant au carré, il viendra

(6) $$x^2 \equiv 2 + i + i^2 \equiv 1 + i,$$

et, en éliminant i entre (5) et (6),

$$x^2 - x + 3 \equiv 0 \pmod{7}.$$

Telle est la congruence irréductible dont dépend la racine primitive demandée. Si l'on représente par i cette racine, les 48 racines de la congruence (1) seront les valeurs des puissances

$$i,\quad i^2,\quad i^3,\quad \ldots,\quad i^{48},$$

réduites par le moyen de la congruence

$$i^2 - i + 3 \equiv 0 \pmod{7}.$$

374. *De la congruence* $x^{7^3-1} - 1 \equiv 0 \pmod{7}$. — Le théorème du n° 358 indique, pour le module 7, l'existence des quatre fonctions irréductibles du troisième degré

$$x^3 - 2,\quad x^3 - 3,\quad x^3 + 3,\quad x^3 + 2.$$

Nous désignerons par i une racine de la congruence

$$i^3 \equiv 2 \pmod{7},$$

et alors les racines de la proposée seront de la forme

$$a_0 + a_1 i + a_2 i^2.$$

Cherchons une racine primitive de la congruence proposée qui est

(1) $$x^{342} - 1 \equiv 0 \quad \text{ou} \quad x^{2.3^2.19} - 1 \equiv 0 \pmod{7}.$$

Il suffit pour cela d'avoir une racine primitive de chacune des trois suivantes :

(2) $$x^2 - 1 \equiv 0,\quad x^{3^2} - 1 \equiv 0,\quad x^{19} - 1 \equiv 0 \pmod{7}.$$

La racine primitive de la première des congruences (2) est -1; la deuxième de ces congruences (2) peut se mettre sous la forme

$$(x^3-1)(x^3-2)(x^3+3)\equiv 0 \pmod{7},$$

et ses racines primitives sont les racines des deux congruences

$$x^3\equiv 2,\quad x^3\equiv -3 \pmod{7};$$

donc i est racine primitive de la deuxième des congruences (2). Il reste à trouver une racine de $x^{19}-1\equiv 0$, ou plutôt de

$$\frac{x^{19}-1}{x-1}\equiv 0 \pmod{7}.$$

Examinons si l'on peut satisfaire à cette congruence en posant simplement $x=a_0+a_1 i$ au lieu de $a_0+a_1 i+a_2 i^2$; nous devrons avoir

$$(a_0+a_1 i)^{19}\equiv 1 \pmod{7},$$

ce qui, en développant par la formule du binôme, et réduisant les puissances de a_0, a_1 et i par les formules

$$a_0^{6m}\equiv 1,\quad a_1^{6m}\equiv 1,\quad i^3\equiv 2 \pmod{7},$$

se réduit à

$$3[a_0-a_0^4 a_1^3+(a_0^5 a_1^2+a_0^2 a_1^5)i^2]\equiv 1,$$

d'où, en séparant,

$$3a_0-3a_0^4 a_1^3\equiv 1,\quad a_0^5 a_1^2+a_0^2 a_1^5\equiv 0.$$

Ces deux dernières conditions sont satisfaites en posant

$$a_0\equiv -1,\quad a_1\equiv +1.$$

Donc $-1+i$ est une racine primitive de la troisième des congruences (2). Le produit des trois quantités

$$-1,\quad i,\quad -1+i,$$

qui est

$$i-i^2,$$

sera donc une racine primitive de la congruence proposée

$$x^{7^3} - 1 \equiv 0 \pmod{7};$$

par conséquent, cette expression jouit de la propriété qu'en l'élevant à toutes les puissances on obtiendra $7^3 - 1$ expressions différentes et de la forme

$$a_0 + a_1 i + a_2 i^2.$$

Si l'on veut connaître la congruence irréductible dont dépend la racine que nous venons de trouver, il faudra éliminer i entre

$$x = i - i^2 \quad \text{et} \quad i^3 \equiv 2 \pmod{7}.$$

En élevant la valeur de x au cube, puis réduisant les exposants de i, il vient

$$x^3 \equiv -2 + i - i^2 \pmod{7},$$

d'où

$$x^3 - x + 2 \equiv 0 \pmod{7}.$$

Il sera convenable de prendre pour *base* des imaginaires et de représenter par i la racine de cette congruence, en sorte que l'on aura

$$i^3 - i + 2 \equiv 0 \pmod{7},$$

et l'on obtiendra toutes les imaginaires de la forme

$$a_0 + a_1 i + a_2 i$$

en élevant i à toutes les puissances et réduisant par la précédente congruence.

375. *De la congruence* $x^{7^4-1} - 1 \equiv 0 \pmod{7}$. — Le théorème du n° 354 nous fait connaître une fonction irréductible du quatrième degré, suivant le module 7, savoir :

$$\frac{x^5 - 1}{x - 1} \quad \text{ou} \quad x^4 + x^3 + x^2 + x + 1;$$

effectivement le module 7 est racine primitive pour le nombre premier 5. En outre, d'après le théorème démontré au n° 358, chacune des trois fonctions binômes

$$x^{16}+1,\quad x^{16}+2,\quad x^{16}-3$$

est décomposable suivant le module 7 en quatre facteurs irréductibles du quatrième degré. On trouve par l'analyse du n° 359 que ces facteurs sont respectivement

$$\begin{array}{lll} x^4+\ x^2-1, & x^4+2x^2-2, & x^4+\ x^2+3, \\ x^4-\ x^2-1, & x^4-2x^2-2, & x^4-\ x^2+3, \\ x^4+3x^2-1, & x^4+3x^2-2, & x^4+2x^2+3, \\ x^4-3x^2-1, & x^4-3x^2-2, & x^4-2x^2+3. \end{array}$$

Nous désignerons par i une racine de la congruence

(1) $$i^4+3i^2-2\equiv 0 \pmod{7},$$

et nous chercherons une racine primitive de la congruence

(2) $$x^{7^4-1}-1\equiv 0 \quad \text{ou} \quad x^{2400}-1\equiv 0 \pmod{7}.$$

Comme $2400=2^5.3.5^2=32\times 3\times 25$, il nous faut connaître une racine primitive de chacune des trois congruences

(3) $$x^{32}-1\equiv 0,\quad x^3-1\equiv 0,\quad x^{25}-1\equiv 0 \pmod{7}.$$

Or la congruence (1) donne

(4) $$\left.\begin{array}{l} i^4\equiv 2-3i^2 \\ i^8\equiv 1+3i^3 \\ i^{16}\equiv -2 \end{array}\right\} \pmod{7}$$

et, par suite,

$$(i^{16})^3=(i^3)^{16}\equiv -1 \pmod{7}.$$

Il résulte de là que i^3 est une racine primitive de la première des congruences (3); la deuxième congruence (3)

admet 2 comme racine primitive; il reste donc à connaître une racine primitive de la troisième

$$x^{25} \equiv 1 \pmod{7};$$

essayons d'y satisfaire en posant

$$x = ai + bi^2;$$

en substituant cette valeur, réduisant au moyen des formules (4) et égalant ensuite à zéro les coefficients des puissances de i, il vient

$$\left.\begin{array}{r} -2a^4b + 3a^2b^3 - b^5 \equiv 0 \\ 2a^5 + 3a^3b^2 - 2ab^4 \equiv 0 \\ -a^4b + 2a^2b^3 - b^5 + 1 \equiv 0 \\ -3a^5 - 2a^3b^2 + ab^4 + 1 \equiv 0 \end{array}\right\} \pmod{7},$$

congruences auxquelles on satisfait en posant $a = 3$, $b = 2$. Ainsi $3i + 2i^2$ est une racine primitive de $x^{25} - 1 \equiv 0$, car il est facile de s'assurer qu'elle ne satisfait pas à $x^5 - 1 \equiv 0$. La congruence proposée admet donc la racine primitive

$$x = 2i^3(3i + 2i^2) = -i^4 - 3i^5,$$

ou, en réduisant,

(5) $$x = -2 + i + 3i^2 + 2i^3.$$

On tire de là

(6) $$\left\{\begin{array}{l} x^2 = -1 - i + i^2 - 3i^3, \\ x^3 = -1 + i - 3i^2 + 2i^3, \\ x^4 = 3 - 3i + i^3, \end{array}\right.$$

et, en éliminant i, on trouve

(7) $$x^4 - 2x^3 - 2x - 2 \equiv 0 \pmod{7}.$$

Si l'on désigne maintenant par i une racine de cette

congruence (7), les 2400 premières puissances de i donneront toutes les racines de la congruence

$$x^{2400} - 1 \equiv 0 \pmod{7}.$$

376. A l'égard des fonctions irréductibles de degré supérieur à 4 pour le module 7, je me bornerai, en terminant, à des indications que le lecteur pourra développer sans difficulté. Nous n'avons aucun théorème qui nous permette de former directement une fonction irréductible du cinquième degré relativement au module 7. Mais il est aisé d'en obtenir une par tâtonnements. Ainsi on reconnaît que la fonction

$$x^5 + x - 3$$

est irréductible suivant le module 7, parce que, si le contraire avait lieu, cette fonction aurait un diviseur du premier ou du deuxième degré, lequel appartiendrait, en même temps, à la fonction $x^{48} - 1$; or il est facile de s'assurer que cette fonction et la proposée n'ont aucun diviseur commun suivant le module 7. Il y a plus, la fonction $x^5 + x - 3$ appartient à l'exposant $7^5 - 1$, en sorte que, si l'on désigne par i une racine de la congruence irréductible

$$i^5 + i - 3 \equiv 0 \pmod{7},$$

les $7^5 - 1$ premières puissances de i donneront les racines de la congruence

$$x^{7^5-1} - 1 \equiv 0 \pmod{7}.$$

Dans le sixième degré, il y a deux fonctions binômes irréductibles, savoir : $x^6 + 2$ et $x^6 - 3$, et il est facile de conclure de l'une ou de l'autre une racine primitive de la congruence

$$x^{7^6-1} - 1 \equiv 0 \pmod{7}.$$

Par exemple, si l'on pose

$$i^6 \equiv -2 \pmod{7},$$

il suffira de déterminer une racine primitive de chacune des quatre congruences

$$x^{16}-1\equiv 0,\quad x^9-1\equiv 0,\quad x^{19}-1\equiv 0,\quad x^{43}-1\equiv 0 \pmod{7},$$

en procédant comme nous l'avons fait dans les cas que nous avons examinés précédemment. On reconnaît facilement que $1+i$ est une racine primitive de la congruence proposée; cette racine appartient à la congruence irréductible

$$(x-1)^6+2\equiv 0 \pmod{7}.$$

Enfin, dans le septième degré, nous connaissons une fonction irréductible, par le théorème du n° 360, savoir : x^7-x-g, g étant différent de zéro. Si l'on désigne par i une racine de la congruence irréductible

$$i^7-i-3\equiv 0 \pmod{7},$$

on reconnaîtra facilement que i est racine primitive pour la congruence

$$x^{7^7-1}-1\equiv 0 \pmod{7}.$$

CHAPITRE IV.

DÉTERMINATION DES FONCTIONS ENTIÈRES IRRÉDUCTIBLES, SUIVANT UN MODULE PREMIER, DANS LE CAS OU LE DEGRÉ EST UNE PUISSANCE DU MODULE.

Sur les fonctions entières irréductibles, suivant un module premier, dans le cas où le degré est égal au module.

377. Dans un travail qui fait partie du tome XXXV des *Mémoires de l'Académie des Sciences*, et dont mon *Algèbre supérieure* reproduit les résultats, j'ai montré qu'on peut obtenir immédiatement une fonction entière du degré ν irréductible suivant le module premier p, lorsque le nombre ν ne renferme aucun facteur premier différent de ceux qui divisent $p-1$, et aussi lorsque ce degré est précisément égal au module.

Je me propose ici de revenir sur le dernier de ces deux cas et d'exécuter la décomposition de la fonction $x^{p^p}-x$ en facteurs irréductibles suivant le module p. Posons

$$(1)\quad \left\{\begin{aligned} X_\mu = x^{p^\mu} - \frac{\mu}{1}x^{p^{\mu-1}} + \ldots + (-1)^k \frac{\mu(\mu-1)\ldots(\mu-k+1)}{1.2\ldots k} x^{p^{\mu-k}} + \ldots \\ + (-1)^{\mu-1}\frac{\mu}{1}x^p + (-1)^\mu x, \end{aligned}\right.$$

il est évident que l'on aura

$$(2)\qquad X_{\mu+1} \equiv X_\mu^p - X_\mu \pmod{p}.$$

Multiplions entre elles les $p-1$ congruences comprises

dans la formule (2) quand on attribue à μ les valeurs 1, 2, 3, ...$(p-1)$, et divisons ensuite la congruence résultante par $X_2 X_3 \ldots X_{p-1}$, il viendra

$$(3)\quad X_p \equiv X_1 (X_1^{p-1}-1)(X_2^{p-1}-1)\ldots(X_{p-1}^{p-1}-1) \quad (\text{mod.}\, p);$$

mais la formule (1) donne

$$X_1 = x^p - x, \quad \text{et} \quad X_p \equiv x^{p^p} - x \quad (\text{mod.}\, p),$$

en sorte que le quotient V de X_p par X_1 est égal au produit de toutes les fonctions entières irréductibles de degré p; on a, par la formule (3),

$$(4)\quad V \equiv (X_1^{p-1}-1)(X_2^{p-1}-1)\ldots(X_{p-1}^{p-1}-1) \quad (\text{mod.}\, p),$$

et l'on sait d'ailleurs que

$$(5)\quad X_\mu^{p-1} - 1 \equiv (X_\mu - 1)(X_\mu - 2)\ldots(X_\mu - \overline{p-1}) \quad (\text{mod.}\, p).$$

Ainsi chacun des facteurs $X_\mu^{p-1}-1$ de V est, d'après la formule (5), le produit de $p-1$ facteurs $X_\mu - g$, où g a les valeurs 1, 2, ... $(p-1)$, et chacun de ces facteurs $X_\mu - g$ est lui-même le produit de $p^{\mu-1}$ facteurs irréductibles du degré p. En particulier, le facteur $X_1^{p-1}-1$ est le produit des $p-1$ polynômes irréductibles

$$(6)\quad x^p - x - g,$$

que j'ai considérés précédemment.

378. Les fonctions entières irréductibles du degré p peuvent être distinguées en $p-1$ genres, en comprenant dans le $\mu^{\text{ième}}$ genre toutes celles dont $X_\mu^{p-1}-1$ est le produit. Le premier genre comprend les $p-1$ fonctions (6).

Soit i une racine de la congruence irréductible

$$(7)\quad i^p - i - 1 \equiv 0 \quad (\text{mod.}\, p),$$

les racines de cette congruence seront

$$i,\quad i+1,\quad i+2,\quad \ldots,\quad i+p-1,$$

et il est évident que les p racines de la congruence

$$x^p - x - g \equiv 0 \pmod{p}$$

seront

$$gi,\quad g(i+1),\quad g(i+2),\quad \ldots,\quad g(i+p-1),$$

en sorte que les fonctions irréductibles du premier genre sont caractérisées par cette circonstance que leurs *racines* sont des fonctions linéaires de i.

Je dis que généralement *les fonctions du $\mu^{\text{ième}}$ genre ont pour racines des fonctions entières de i du degré μ.*

En effet, considérons une telle fonction, et désignons par

$$(8) \qquad f(i) = a_0 + a_1 i + a_2 i^2 + \ldots + a_{p-1} i^{p-1}$$

l'une des racines de la congruence obtenue en l'égalant à zéro, suivant le module p. D'après ce qui a été dit plus haut, $f(i)$ sera racine de la congruence $X_\mu \equiv g \pmod{p}$, dans laquelle g a une valeur convenable. Exécutant la substitution et observant que

$$[f(i)]^{p^m} \equiv f(i^{p^m}) \equiv f(i+m) \pmod{p},$$

il viendra

$$f(i+\mu) - \frac{\mu}{1} f(i+\mu-1) + \frac{\mu(\mu-1)}{1.2} f(i+\mu-2) - \ldots$$
$$+ (-1)^{\mu-1} \frac{\mu}{1} f(i+1) + (-1)^\mu f(i) \equiv g \pmod{p}.$$

Cette congruence est nécessairement identique, car son premier membre est un polynôme en i de degré in-

férieur à p; d'ailleurs ce premier membre est la différence $\mu^{\text{ième}}$ de $f(i)$ relative à la différence constante 1 attribuée à i; donc, puisqu'il se réduit à la constante g différente de zéro, le degré de $f(i)$ est précisément égal à μ; on a, en conséquence,

$$a_\mu = \frac{g}{1.2\ldots\mu} \quad \text{et} \quad a_{\mu+1} = a_{\mu+2} = \ldots = a_{p-1} = 0.$$

379. Il est aisé d'obtenir les fonctions irréductibles des différents genres. Supposons que les p coefficients $a_0, a_1, \ldots, a_{p-1}$ de la formule (8) restent indéterminés, en excluant le cas où $f(i)$ se réduirait à la constante a_0, et considérons la congruence

$$(9) \qquad i^\lambda[f(i) - x] \equiv 0 \pmod{p},$$

dans laquelle λ prendra les p valeurs $0, 1, 2, \ldots, p-1$. Si l'on rabaisse au-dessous de p les exposants de i, en faisant usage de la congruence (7), la formule (9) donnera p congruences, dont les premiers membres seront des fonctions homogènes et linéaires des puissances $i^0, i^1, i^2, \ldots, i^{p-1}$. En égalant à zéro, suivant le module p, le déterminant $F(x)$ formé avec les coefficients de ces puissances de i, on obtiendra la congruence irréductible dont les racines sont

$$(10) \qquad f(i), \quad f(i+1), \ldots, \quad f(i+p-1);$$

$F(x)$ sera donc une fonction entière irréductible du degré p.

Si l'on fait, pour abréger l'écriture,

$$a_k + a_{k-1} = a'_k,$$

et qu'on regarde a_p comme équivalent à a_0, en sorte

que a'_0 représente $a_0 + a_{p-1}$, on trouve immédiatement

$$(11)\quad F(x) = -\begin{vmatrix} a_0 - x & a_1 & a_2 & \ldots & a_{p-3} & a_{p-2} & a_{p-1} \\ a_{p-1} & a'_0 - x & a_1 & \ldots & a_{p-4} & a_{p-3} & a_{p-2} \\ a_{p-2} & a'_{p-1} & a'_0 - x & \ldots & a_{p-5} & a_{p-4} & a_{p-3} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_3 & a'_4 & a'_5 & \ldots & a'_0 - x & a_1 & a_2 \\ a_2 & a'_3 & a'_4 & \ldots & a'_{p-2} & a'_0 - x & a_1 \\ a_1 & a'_2 & a'_3 & \ldots & a'_{p-2} & a'_{p-1} & a'_0 - x \end{vmatrix}.$$

Telle est l'expression générale des fonctions irréductibles du degré p suivant le module p.

Si l'on veut avoir les fonctions du $\mu^{\text{ième}}$ genre, on fera

$$(12)\qquad a_{\mu+1} = 0,\quad a_{\mu+2} = 0,\quad \ldots,\quad a_{p-1} = 0,$$

et l'on peut supposer aussi

$$(13)\qquad a_{\mu-1} = 0.$$

En effet, la congruence $F(x) \equiv 0 \pmod{p}$ est celle dont dépendent les racines (10); or, parmi ces expressions (10), il y en a une, $f(i+\lambda)$, dans laquelle le coefficient de $i^{\mu-1}$ est congru à zéro, et rien n'empêche de substituer dans notre analyse $f(i+\lambda)$ à $f(i)$.

Ayant donc égard aux équations (12) et (13), si l'on attribue aux coefficients $a_0, a_1, \ldots, a_{\mu-2}$ les valeurs $0, 1, 2, \ldots, p-1$ et à a_μ les mêmes valeurs, zéro excepté, la formule (11) fera connaître les $(p-1)p^{\mu-1}$ fonctions irréductibles du $\mu^{\text{ième}}$ genre.

Si on fait l'application au cas de $\mu = 1$ et à celui de $\mu = 2$, on trouvera :

1° Pour $\mu = 1$, $F(x) = x^p - x - a_1$;

2° Pour $\mu = 2$, $F(x) = (x - a_0)\left[(x-a_0)^{\frac{p-1}{2}} - a_2^{\frac{p-1}{2}}\right]^2 - a_2$.

380. Parmi les fonctions du $(p-1)^{\text{ième}}$ genre, il faut remarquer celles qui répondent au cas où les coefficients de la formule (8) sont nuls, à l'exception de a_0 et a_{p-1}; ces fonctions ont pour expression

$$F(x) = (x - a'_0)^p + a_{p-1}[(x - a'_0)^{p-1} - 1],$$

et elles ont cette propriété que les racines de la congruence $F(x) \equiv 0 \pmod{p}$ sont des fonctions rationnelles et linéaires de l'une d'entre elles. Effectivement, la congruence dont il s'agit peut, si l'on y introduit la racine a'_0, se mettre sous la forme

$$x^p \equiv \frac{(a_{p-1} + a'_0)x - a'^2_0}{x + (a_{p-1} - a'_0)} \pmod{p},$$

et l'on sait d'ailleurs que ses racines peuvent être représentées par x, x^p, x^{p^2}, ..., $x^{p^{p-1}}$.

Sur les fonctions entières irréductibles suivant un module premier, dans le cas où le degré est une puissance du module.

381. Je me propose d'examiner ici le cas plus général des fonctions entières irréductibles, dont le degré est égal à une puissance quelconque du module premier p.

Posons, comme dans le précédent article,

$$\left\{\begin{aligned} X_\mu \equiv x^{p^\mu} - \frac{\mu}{1} x^{p^{\mu-1}} + \ldots + (-1)^k \frac{\mu(\mu-1)\ldots(\mu-k+1)}{1.2\ldots k} x^{p^{\mu-k}} + \ldots \\ + (-1)^{\mu-1} \frac{\mu}{1} x^p + (-1)^\mu x \pmod{p}, \end{aligned}\right.$$

formule de laquelle résulte la congruence

$$(2) \qquad X_{\mu+1} \equiv X_\mu^p - X_\mu \pmod{p}.$$

La formule (1) peut s'écrire *symboliquement* de la manière suivante :

$$X_\mu \equiv (\xi - 1)^\mu \pmod{p},$$

en convenant que, après avoir effectué l'opération indiquée dans le second membre, on remplacera chaque puissance $\xi^{\mu-k}$ de ξ par $x^{p^{\mu-k}}$. Alors, si l'indice μ est divisible par une puissance de p, et que l'on fasse

$$\mu = \nu p^m,$$

on aura symboliquement

$$X_{\nu p^m} \equiv (\xi - 1)^{\nu p^m} \equiv [(\xi - 1)^{p^m}]^\nu \equiv (\xi^{p^m} - 1)^\nu \pmod{p},$$

c'est-à-dire

$$(3)\quad \begin{cases} X_{\nu p^m} \equiv x^{p^{\nu p^m}} - \frac{\nu}{1} x^{p^{(\nu-1)p^m}} + \ldots + (-1)^k \frac{\nu(\nu-1)\ldots(\nu-k+1)}{1.2\ldots k} x^{p^{(\nu-k)p^m}} + \ldots \\ \quad + (-1)^{\nu-1} \frac{\nu}{1} x^{p^{p^m}} + (-1)^\nu x \pmod{p}; \end{cases}$$

dans le cas de $\nu = 1$, on a

$$(4)\qquad X_{p^m} \equiv x^{p^{p^m}} - x \pmod{p}.$$

La formule (2) exprime que X_μ se change en $X_{\mu+1}$ quand on change x en $x^p - x$; d'ailleurs la même formule se réduit, pour $\mu = 0$, à

$$X_1 = X_0^p - X_0,$$

ce qui montre qu'on doit regarder X_0 comme étant égal à x. Il résulte de là que, pour exécuter ρ fois de suite, dans les formules (1) et (3), le changement de x en $x^p - x$, il suffit d'ajouter ρ unités aux indices des fonc-

tions X qui y figurent. La formule (3) devient ainsi

$$\ldots_{m+\rho} \equiv X_\rho^{p^{\nu p^m}} - \frac{\nu}{1} X_\rho^{p^{(\nu-1)p^m}} + \ldots + (-1)^k \frac{\nu(\nu-1)\ldots(\nu-k+1)}{1.2\ldots k} X_\rho^{p^{(\nu-k)p^m}} + \ldots$$

$$+ (-1)^{\nu-1} \frac{\nu}{1} X_\rho^{p^{p^m}} + (-1)^\nu X_\rho \pmod{p}.$$

382. Je désignerai généralement par V_n le produit de toutes les fonctions entières de degré p^n, irréductibles suivant le module p. D'après la formule (4), ce produit est égal au quotient des deux fonctions X_{p^n}, $X_{p^{n-1}}$; ainsi l'on a

$$(6) \qquad X_{p^n} \equiv X_{p^{n-1}} V_n \pmod{p}.$$

Ensuite la formule (2) donne

$$\left.\begin{array}{l} X_{\mu+1} \equiv X_\mu^p \quad - X_\mu, \\ X_{\mu+2} \equiv X_{\mu+1}^p \quad - X_{\mu+1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ X_{\mu+\nu} \equiv X_{\mu+\nu-1}^p - X_{\mu+\nu-1} \end{array}\right\} \pmod{p};$$

multipliant ces congruences entre elles et divisant la formule résultante par le produit $X_{\mu+1} X_{\mu+2} \ldots X_{\mu+\nu-1}$, il vient

$$(7) \quad X_{\mu+\nu} \equiv X_\mu (X_\mu^{p-1} - 1)(X_{\mu+1}^{p-1} - 1)\ldots(X_{\mu+\nu-1}^{p-1} - 1) \pmod{p}.$$

Faisons

$$\mu = p^{n-1}, \quad \mu + \nu = p^n,$$

il viendra, à cause de la formule (6),

$$V_n \equiv (X_{p^{n-1}}^{p-1} - 1)(X_{p^{n-1}+1}^{p-1} - 1)(X_{p^{n-1}+2}^{p-1} - 1)\ldots(X_{p^n-1}^{p-1} - 1) \pmod{p}.$$

Chacun des facteurs $X_{p^{n-1}+\lambda-1}^{p-1} - 1$ du second membre de la formule (8) se décompose en $p-1$ facteurs

$X_{p^{n-1}+\lambda-1} - g$, où g a les valeurs $1, 2, \ldots, p-1$, et cette dernière fonction est elle-même le produit de $p^{p^{n-1}+\lambda-n-1}$ facteurs irréductibles du degré p^n.

Il y a lieu de distinguer en plusieurs genres les fonctions entières irréductibles de degré p^n, ainsi que je l'ai fait déjà dans le cas particulier de $n=1$. Je nommerai fonctions du $\lambda^{\text{ième}}$ genre celles dont $X^{p-1}_{p^{n-1}+\lambda-1} - 1$ est le produit, λ ayant les valeurs

$$1,\quad 2,\quad 3,\quad \ldots,\quad (p-1)p^{n-1},$$

et le dernier genre, celui qui répond à $\lambda = (p-1)p^{n-1}$, sera dit le *genre principal*.

Si l'on exécute le changement de x en $x^p - x$, dans le second membre de la formule (8), chacun des $p^n - p^{n-1} - 1$ premiers facteurs entre parenthèses se changera dans le facteur suivant, d'après ce qui a été dit plus haut. Quant au dernier facteur $X^{p-1}_{p^n-1} - 1$, qui est le produit des fonctions irréductibles du genre principal, il se changera en $X^{p-1}_{p^n} - 1$, ce qui est le premier facteur de V_{n+1}, c'est-à-dire le produit des fonctions entières irréductibles du degré p^{n+1} et du premier genre. De cette considération résulte immédiatement le théorème suivant :

Théorème. — *Soit* $F(x)$ *une fonction entière du degré* p^n, *irréductible suivant le module premier* p. *Si cette fonction appartient au* $\lambda^{\text{ième}}$ *genre supposé non principal, la fonction* $F(x^p - x)$ *ou* $F(X_1)$ *sera réductible, et elle se décomposera en* p *facteurs du degré* p^n, *irréductibles suivant le module* p *et appartenant au* $(\lambda+1)^{\text{ième}}$ *genre. Mais, si la fonction* $F(x)$ *de degré* p^n *appartient au genre principal, la fonction* $F(x^p - x)$ *sera elle-même irréductible suivant le module* p, *et elle appartiendra au premier genre des fonctions de degré* p^{n+1}.

383. Considérons d'abord les fonctions entières irréductibles de degré p^n et du premier genre. Le produit de ces fonctions est

$$X_{p^{n-1}}^{p-1} - 1 \equiv \Pi(X_{p^{n-1}} - g) \pmod{p},$$

le signe de produit Π s'étendant aux valeurs 1, 2, ..., $(p-1)$ de g. Le facteur $X_{p^{n-1}} - g$ est ce que devient $X_{p^{n-1}} - 1$ quand on y remplace x par $\frac{x}{g}$ et qu'on multiplie le résultat par g; il s'ensuit que la recherche des fonctions entières irréductibles du premier genre est ramenée à la décomposition en facteurs de la seule expression

$$(9) \qquad X_{p^{n-1}} - 1 \equiv x^{p^{p^{n-1}}} - x - 1 \pmod{p}.$$

Soient $F(x)$ l'un des facteurs irréductibles de la fonction (9) et i_n une racine de la congruence

$$(10) \qquad F(x) \equiv 0 \pmod{p}.$$

La racine i_n appartiendra aussi à la congruence

$$(11) \qquad X_{p^{n-1}} - 1 \equiv 0 \pmod{p},$$

et l'on aura en conséquence

$$(12) \qquad i_n^{p^{p^{n-1}}} - i_n \equiv 1 \pmod{p}.$$

En tenant compte de la formule (12), la congruence (11) peut s'écrire de la manière suivante :

$$(x - i_n)^{p^{p^{n-1}}} - (x - i_n) \equiv 0 \pmod{p},$$

et, par conséquent, les $p^{p^{n-1}}$ racines de cette congruence seront données par la formule

$$(13) \qquad x \equiv i_n + f(i_{n-1}) \pmod{p},$$

dans laquelle i_{n-1} désigne une racine d'une congruence

irréductible quelconque de degré p^{n-1}, et f une fonction entière du degré $p^{n-1}-1$, dont les coefficients peuvent avoir les valeurs $0, 1, 2, \ldots, (p-1)$.

Parmi les valeurs de x comprises dans la formule (13), figurent les p^n racines de la congruence (10), et comme, d'après la théorie des congruences, l'une de ces racines est i_n^p, on aura

$$(14) \qquad i_n^p - i_n \equiv f(i_{n-1}) \pmod{p},$$

la fonction f devant être ici convenablement choisie. La formule (14) permet d'éliminer des expressions qui contiennent les puissances de i_n au delà de la $(p-1)^{\text{ième}}$, en introduisant les diverses puissances de i_{n-1}.

De là on peut conclure que, si l'on désigne par

$$i_1, \; i_2, \; i_3, \; \ldots, \; i_n$$

des racines de congruences irréductibles suivant le module p, dont les premiers membres soient des diviseurs des fonctions respectives

$$X_1 - 1, \quad X_p - 1, \quad X_{p^2} - 1, \quad \ldots, \quad X_{p^{n-1}} - 1,$$

on aura

$$(15) \qquad \left\{\begin{array}{l} i_1^p - i_1 \equiv 1, \\ i_2^p - i_2 \equiv P_1, \\ i_3^p - i_3 \equiv P_2, \\ \ldots\ldots\ldots\ldots, \\ i_n^p - i_n \equiv P_{n-1} \end{array}\right\} \pmod{p},$$

P_μ étant une fonction entière des racines $i_1, i_2, \ldots, i_\mu$, qui ne renferme aucune puissance de ces racines supérieure à la $(p-1)^{\text{ième}}$.

Il reste à connaître la condition que doivent remplir les fonctions P_μ pour que les valeurs de $i_1, i_2, \ldots, i_n$,

définies par les formules (15), satisfassent effectivement aux congruences respectives

$$X_1 - 1 \equiv 0,\ X_p - 1 \equiv 0,\ X_{p^2} - 1 \equiv 0, \ldots,\ X_{p^{n-1}} - 1 \equiv 0 \pmod{p}.$$

Pour remplir cet objet, nous aurons à nous appuyer sur un lemme que nous allons d'abord établir.

384. **Lemme.** — *Soit*

$$f(\zeta) = a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_\nu\zeta^\nu$$

une fonction entière du degré $\nu < p$, d'une quantité ζ racine de la congruence

$$\zeta^{p^{p^m}} - \zeta \equiv 1 \pmod{p},$$

et dont les coefficients a, réels ou imaginaires, satisfont tous à la congruence

$$a^{p^{p^m}} - a \equiv 0 \pmod{p};$$

si l'on attribue à X_ρ la valeur $f(\zeta)$, on aura

$$X_{\nu p^m + \rho} \equiv 1.2\ldots\nu.a_\nu \pmod{p}.$$

La démonstration de ce lemme se déduit très-facilement de la formule (5), qui donne l'expression de $X_{\nu p^m+\rho}$ en fonction de X_ρ. Pour élever $f(\zeta)$ à la puissance $p^{(\nu-k)p^m}$, il faut répéter $\nu - k$ fois l'opération de l'élévation à la puissance p^{p^m}; or, d'après l'énoncé du lemme, cette opération change ζ en $\zeta + 1$ et elle laisse invariables les coefficients a; donc l'hypothèse $X_\rho = f(\zeta)$ entraîne

$$X_\rho^{p^{(\nu-k)p^m}} \equiv f(\zeta + \nu - k) \pmod{p},$$

et, à cause de la formule (5),

$$\left.\begin{aligned} {}_{m+\rho} \equiv f(\zeta+\nu) - \frac{\nu}{1} f(\zeta+\nu-1) + \frac{\nu(\nu-1)}{1.2} f(\zeta+\nu-2) + \ldots \\ + (-1)^{\nu-1}\frac{\nu}{1} f(\zeta+1) + (-1)^\nu f(\zeta) \end{aligned}\right\} \pmod{p}.$$

Le second membre de cette congruence est la différence $\nu^{\text{ième}}$ de la fonction $f(\zeta)$ relative à la différence constante 1 attribuée à ζ; il a donc pour valeur

$$1.2\ldots\nu.a_\nu,$$

ce qui démontre la proposition énoncée.

Comme le produit $1.2.3\ldots(p-1)$ est congru à -1, suivant le module p, on déduit de ce qui précède le corollaire suivant, relatif au cas de $\nu = p-1$.

Corollaire. — *Si l'on attribue à X_ρ une valeur représentée par une fonction entière $f(\zeta)$ du degré $p-1$, d'une racine ζ de la congruence $\zeta^{p^{p^m}} - \zeta \equiv 1 \pmod{p}$, dont les coefficients a satisfassent à la congruence $a^{p^{p^m}} - a \equiv 0 \pmod{p}$, la fonction $X_{p^{m+1}-p^{m}+\rho}$ prendra une valeur congrue au coefficient changé de signe de la puissance ζ^{p-1} dans $f(\zeta)$.*

385. Revenons maintenant aux formules (15). Supposons les fonctions

$$P_1,\ P_2,\ \ldots,\ P_{n-2},$$

telles que $i_1, i_2, \ldots, i_{n-1}$ soient respectivement racines des $n-1$ premières congruences (16), et cherchons dans quel cas la valeur de i_n, définie par la dernière des formules (15), est racine de la dernière des congruences (16). Il est évident que cela revient à chercher dans quel cas la congruence

$$X_1 \equiv P_{n-1} \pmod{p}$$

entraîne

$$X_{p^{n-1}} \equiv 1 \pmod{p}.$$

Désignons par $P_{n-1}^{(1)}$ le coefficient de i_{n-1}^{p-1} dans P_{n-1}, par $P_{n-1}^{(2)}$ le coefficient de i_{n-2}^{p-1} dans $P_{n-1}^{(1)}$, par $P_{n-1}^{(3)}$ le coefficient de i_{n-3}^{p-1} dans $P_{n-1}^{(2)}$, et ainsi de suite; le coefficient $P_{n-1}^{(n-1)}$ de i_1 dans $P_{n-1}^{(n-2)}$ sera un nombre entier.

Cela posé, le corollaire du lemme du n° 384 est applicable successivement dans les $n-1$ hypothèses suivantes :

$$\begin{array}{llll}
= n-2, & \rho = 1, & \zeta = i_{n-1}, & f(\zeta) = +\mathrm{P}_{n-1}, \\
= n-3, & \rho = p^{n-1} - p^{n-2} + 1, & \zeta = i_{n-2}, & f(\zeta) = -\mathrm{P}_{n-1}^{(1)}, \\
= n-4, & \rho = p^{n-1} - p^{n-3} + 1, & \zeta = i_{n-3}, & f(\zeta) = +\mathrm{P}_{n-1}^{(2)}, \\
= n-5, & \rho = p^{n-1} - p^{n-4} + 1, & \zeta = i_{n-4}, & f(\zeta) = -\mathrm{P}_{n-1}^{(3)}, \\
\ldots\ldots, & \ldots\ldots\ldots\ldots, & \ldots\ldots, & \ldots\ldots\ldots\ldots, \\
= 0, & \rho = p^{n-1} - p + 1, & \zeta = i_1, & f(\zeta) = (-1)^{n-2}\mathrm{P}_{n-1}^{(n-2)}.
\end{array}$$

Effectivement les conditions de ce corollaire, savoir :

$$\zeta^{p^{p^m}} - \zeta \equiv 1, \quad a^{p^{p^m}} - a \equiv 0 \pmod{p},$$

sont remplies dans chacune de nos $n-1$ hypothèses; donc la congruence

$$\mathrm{X}_1 \equiv \mathrm{P}_{n-1} \pmod{p}$$

entraînera successivement les suivantes :

$$\left.\begin{array}{ll}
\mathrm{X}_{p^{n-1}-p^{n-2}+1} & \equiv -\mathrm{P}_{n-1}^{(1)} \\
\mathrm{X}_{p^{n-1}-p^{n-3}+1} & \equiv +\mathrm{P}_{n-1}^{(2)}, \\
\mathrm{X}_{p^{n-1}-p^{n-4}+1} & \equiv -\mathrm{P}_{n-1}^{(3)}, \\
\ldots\ldots\ldots\ldots\ldots, & \\
\mathrm{X}_{p^{n-1}-p+1} & \equiv (-1)^{n-2}\mathrm{P}_{n-1}^{(n-2)}, \\
\mathrm{X}_{p^{n-1}} & \equiv (-1)^{n-1}\mathrm{P}_{n-1}^{(n-1)}
\end{array}\right\} \pmod{p},$$

et, par conséquent, pour avoir $\mathrm{X}_{p^{n-1}} \equiv 1 \pmod{p}$, il faut et il suffit que

$$\mathrm{P}_{n-1}^{(n-1)} \equiv (-1)^{n-1} \pmod{p},$$

c'est-à-dire que P_{n-1} contienne le terme $i_1^{p-1} i_2^{p-1} \ldots i_{n-1}^{p-1}$ avec le coefficient $(-1)^{n-1}$.

et nous ferons en outre

$$i_1 i_2 = \frac{1}{z},$$

d'où

$$z^{p-1} \equiv \frac{1}{X_1 + 1} \quad (\text{mod. } p).$$

On tire de ces formules

$$\frac{\frac{1}{z^p}}{i_1^p} \equiv \frac{\frac{1}{z} + 1}{i_1} \equiv \frac{\frac{1}{z^p} - \frac{1}{z} - 1}{1} \quad (\text{mod. } p),$$

d'où

$$i_1 \equiv \frac{1 + z}{X_1 - z}, \quad i_1^p \equiv \frac{X_1 + 1}{X_1 - z} \quad (\text{mod. } p),$$

et l'élimination de i_1 donne

$$\frac{X_1(X_1 + 1)(X_1^p + X_1^{p-1} - 1) - X_1 z + z^2}{z(X_1 - z)} \equiv 0 \quad (\text{mod. } p),$$

ou, en désignant par z_1, z_2 les valeurs de z qui annulent le numérateur,

$$\frac{(z_1 - z)(z_2 - z)}{z(X_1 - z)} \equiv 0 \quad (\text{mod. } p).$$

Multiplions entre elles la précédente congruence et celles qu'on déduit de celle-ci par le changement de z en $2z, 3z, \ldots, (p-1)z$; remplaçons ensuite z^{p-1} par $\frac{1}{X_1 + 1}$; il viendra

$$\frac{(X_1 + 1)^2(z_1 z_2)^{p-1} - (X_1 + 1)(z_1^{p-1} + z_2^{p-1} - X_1^{p-1})}{X_1^p + X_1^{p-1} - 1} - 1 \equiv 0 \quad (\text{mod. } p).$$

Faisons, pour abréger l'écriture,

$$P = X_1(X_1+1)(X_1^p + X_1^{p-1} - 1),$$

$$= X_1^{p-3} + \frac{4}{2} X_1^{p-5} P + \ldots + \frac{(\mu+2)(\mu+3)\ldots 2\mu}{2.3\ldots\mu} X_1^{p-2\mu-1} P^{\mu-1} + \ldots$$

$$+ \frac{\left(\frac{p-1}{2}+2\right)\ldots(p-1)}{2.3\ldots\frac{p-1}{2}} P^{\frac{p-3}{2}},$$

on aura

$$z_1 z_2 \equiv P \qquad z_1^{p-1} + z_2^{p-1} \equiv X_1^{p-1} + PQ \pmod{p},$$

et notre congruence deviendra

$$(X_1+1)^2 X_1 P^{p-2} - (X_1+1)^2 X_1 Q - 1 \equiv 0 \pmod{p}.$$

Le premier membre de cette congruence est une fonction entière irréductible du degré p^3 et du premier genre.

388. Les formules (15) du n° 383 peuvent être regardées comme définissant un premier groupe de fonctions entières irréductibles du premier genre et des degrés respectifs $p, p^2, \ldots, p^n$. Nous allons montrer de quelle manière les fonctions irréductibles du degré p^n des divers genres se rattachent à ce groupe fondamental.

Revenons donc à la formule (8) et considérons l'un quelconque des facteurs de son second membre. Posons

$$(20) \qquad Z_\mu \equiv X_\mu^{p-1} - 1 \pmod{p};$$

l'indice μ a l'une quelconque des valeurs

$$p^{n-1}, \quad p^{n-1}+1, \quad p^{n-1}+2, \quad \ldots, \quad p^n - 1;$$

nous le supposerons mis sous la forme

$$\mu = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \ldots + \alpha_{n-1} p^{n-1},$$

$\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ étant des entiers positifs ou nuls et inférieurs à p.

Désignons par ξ_0 un entier arbitraire, et faisons généralement

$$(21) \quad \xi_{k+1} \equiv a_0^{(k)} + a_1^{(k)} i_{k+1} + a_2^{(k)} i_{k+1}^2 + \ldots + a_{\alpha_k-1}^{(k)} i_{k+1}^{\alpha_k-1} + i_{k+1}^{\alpha_k} \pmod{p},$$

$a_0^k, a_1^k, \ldots$ étant des fonctions entières de $i_1, i_2, \ldots, i_k$ qui se réduisent à des entiers dans le cas de $k = 0$; la quantité ξ_{k+1} se réduira elle-même à l'unité dans le cas de $\alpha_k = 0$. Quant aux racines $i_1, i_2, \ldots, i_n$, elles sont, je le répète, définies par les formules (15).

Cela posé, je dis que les $(p-1)p^\mu$ racines de la congruence

$$(22) \qquad Z_\mu \equiv 0 \pmod{p}$$

sont données par la formule

$$(23) \qquad x \equiv \xi_0 \xi_1 \xi_2 \ldots \xi_n \pmod{p},$$

dont le second membre est effectivement susceptible de $(p-1)p^\mu$ valeurs différentes. Deux de ces valeurs de x sont nécessairement distinctes, car leur différence est une fonction de degré inférieur à p par rapport aux quantités i qui y figurent, et notamment par rapport à celle i_m de ces quantités qui a le plus grand indice. Si donc la différence dont nous parlons était congrue à zéro, i_m serait racine d'une congruence de degré inférieur à p^m, ce qui n'a pas lieu.

D'après cela, il nous suffit de prouver que la valeur (23) de x satisfait à la congruence (22), et nous y parvenons sans difficulté au moyen du lemme du n° 384.

Faisons, pour abréger,

$$\mu_k = \alpha_0 + \alpha_1 p + \ldots + \alpha_k p^k$$

et

$$A_k = 1.2\ldots\alpha_{n-1} \times 1.2\ldots\alpha_{n-2} \times \ldots \times 1.2\ldots\alpha_k;$$

si l'on applique le lemme du n° 384 dans les n hypothèses suivantes :

$$\begin{array}{lllll}
m = n-1, & \nu = \alpha_{n-1}, & \rho = 0, & \zeta = i_n, & f(\zeta) = \xi_0\xi_1\ldots\xi_{n-1}\xi_n, \\
m = n-2, & \nu = \alpha_{n-2}, & \rho = \mu - \mu_{n-2}, & \zeta = i_{n-1}, & f(\zeta) = A_{n-1}\xi_0\xi_1\ldots\xi_{n-1}, \\
m = n-3, & \nu = \alpha_{n-3}, & \rho = \mu - \mu_{n-3}, & \zeta = i_{n-2}, & f(\zeta) = A_{n-2}\xi_0\xi_1\ldots\xi_{n-2}, \\
\ldots\ldots, & \ldots\ldots, & \ldots\ldots, & \ldots\ldots, & \ldots\ldots\ldots\ldots, \\
m = 0, & \nu = \alpha_0, & \rho = \mu - \mu_0, & \zeta = i_1, & f(\zeta) = A_1\xi_0\xi_1,
\end{array}$$

on reconnaîtra que la formule (23) entraîne successivement les suivantes :

$$\left.\begin{array}{ll}
X_{\mu-\mu_{n-2}} \equiv A_{n-1}\,\xi_0\xi_1\ldots\xi_{n-1}, \\
X_{\mu-\mu_{n-3}} \equiv A_{n-2}\xi_0\xi_1\ldots\xi_{n-2}, \\
\ldots\ldots\ldots\ldots\ldots\ldots, \\
X_{\mu-\mu_0} \equiv A_1\xi_0\xi_1, \\
X_\mu \equiv A_0\xi_0
\end{array}\right\} \pmod{p},$$

et, puisque X_μ se réduit ainsi à une constante, il est évident que la congruence (22) est satisfaite.

La formule (23) définit, avec les formules (15), les congruences irréductibles des divers genres de degré p^n. Celles-ci s'obtiennent effectivement en éliminant i_1, $i_2, \ldots, i_n$ de la formule (23). Par les motifs indiqués au n° 386, on peut, en vue de cette élimination, supposer nulle la partie constante du coefficient de l'avant-dernier terme des fonctions ξ.

CHAPITRE V.

SUR LA TOTALITÉ DES NOMBRES PREMIERS COMPRIS ENTRE DES LIMITES DONNÉES.

Sur l'évaluation approchée du produit $1.2.3\ldots x$, *quand* x *est un grand nombre.*

389. La théorie que j'ai surtout en vue dans ce Chapitre exige que l'on connaisse les premiers termes de la série par laquelle on exprime le logarithme du produit des x premiers nombres entiers. Cette série célèbre est celle de Stirling, et elle a fait l'objet des recherches d'un grand nombre de géomètres, parmi lesquels je dois spécialement mentionner Cauchy, Binet, M. Malmsten et M. Liouville. Mais, parmi les démonstrations diverses qu'on possède de cette formule, je ne crois pas qu'il y en ait de plus simple que celle que j'ai présentée à l'Académie des Sciences, dans la séance du 2 avril 1860, et que j'ai reproduite dans une Note qui fait partie de la sixième édition du *Traité élémentaire de Calcul différentiel et intégral* de Lacroix. J'ai montré dans cette Note que la formule connue de Wallis suffit pour établir complétement celle de Stirling, et la déduction est si facile, que la deuxième formule peut en quelque sorte être regardée comme une transformée de la première. Je ne reproduirai pas ici tous les développements que j'ai donnés ailleurs sur ce sujet, et je me bornerai à établir les seuls résultats qui sont indispensables pour l'objet spécial que j'ai en vue.

Rappelons d'abord que la formule de Wallis, qui sera notre point de départ, se déduit de la formule

$$\cos z = \left(1 - \frac{4z^2}{\pi^2}\right)\left(1 - \frac{4z^2}{9\pi^2}\right)\left(1 - \frac{4z^2}{25\pi^2}\right)\cdots,$$

par laquelle on obtient la fonction $\cos z$ décomposée en un produit d'une infinité de facteurs linéaires ([1]). Cette dernière formule peut s'écrire ainsi :

$$\frac{\pi}{2}\,\frac{\sin\left(\frac{\pi}{2} - z\right)}{\frac{\pi}{2} - z} = \left(1 + \frac{2z}{\pi}\right)\left(1 - \frac{4z^2}{9\pi^2}\right)\left(1 - \frac{4z^2}{25\pi^2}\right)\cdots,$$

et en faisant $z = \frac{\pi}{2}$, il vient

$$= 2\left(1 - \frac{1}{9}\right)\left(1 - \frac{1}{25}\right)\left(1 - \frac{1}{49}\right)\cdots\left[1 - \frac{1}{(2x-1)^2}\right] \text{ (pour } x = \infty\text{)},$$

ou

$$\frac{\pi}{2} = \frac{2}{1}\,\frac{2}{3}\,\frac{4}{3}\,\frac{4}{5}\cdots\frac{2x-2}{2x-3}\,\frac{2x-2}{2x-1}\,\frac{2x}{2x-1} \text{ (pour } x = \infty\text{)},$$

ce qui est la formule de Wallis.

390. Cette formule prend la forme très-simple

$$\frac{[\varphi(x)]^4}{[\varphi(2x)]^2} = 1 \quad \text{(pour } x = \infty\text{)},$$

ou, en extrayant la racine carrée,

$$(1) \qquad \frac{[\varphi(x)]^2}{\varphi(2x)} = 1 \quad \text{(pour } x = \infty\text{)},$$

si l'on désigne par $\varphi(x)$, soit l'expression

$$\frac{1.2.3\ldots x}{\sqrt{2\pi}\,x^{x+\frac{1}{2}}},$$

---

(1) *Voir* mon *Traité de Trigonométrie*, 5e édition, p. 244.

soit le produit de cette même expression par une exponentielle de la forme a^x, a étant une constante quelconque. La formule (1) aura donc lieu si, désignant par e la base des logarithmes népériens, on pose

$$(2) \qquad \varphi(x) = \frac{1.2.3\ldots x}{\sqrt{2\pi}\, e^{-x} x^{x+\frac{1}{2}}}.$$

On tire de là la formule (2)

$$(3) \qquad \frac{\varphi(x)}{\varphi(x+1)} = \frac{1}{e}\left(1+\frac{1}{x}\right)^{x+\frac{1}{2}} = e^{-1+\left(x+\frac{1}{2}\right)\log\left(1+\frac{1}{x}\right)},$$

ou

$$(4) \qquad \log\frac{\varphi(x)}{\varphi(x+1)} = -1 + \left(x+\frac{1}{2}\right)\log\left(1+\frac{1}{x}\right),$$

la caractéristique *log* exprimant ici des logarithmes népériens. Or on a, x étant > 1,

$$\log\left(1+\frac{1}{x}\right) = \frac{1}{x} - \frac{1}{2x^2} + \frac{1}{3x^3} - \ldots + \frac{(-1)^{n-1}}{nx^n} + \ldots,$$

d'où

$$\left(x+\frac{1}{2}\right)\log\left(1+\frac{1}{x}\right) = 1 + \frac{1}{12x^2} - \frac{1}{12x^3} + \ldots$$
$$+ \frac{n-1}{2n(n+1)}\frac{(-1)^n}{x^n} + \ldots;$$

donc on a

$$(5) \qquad \begin{cases} \log\dfrac{\varphi(x)}{\varphi(x+1)} = \dfrac{1}{12x^2} - \dfrac{1}{12x^3} + \dfrac{3}{40x^4} - \ldots \\ \qquad\qquad + \dfrac{(n-1)}{2n(n+1)}\dfrac{(-1)^n}{x^n} + \ldots. \end{cases}$$

Dans cette série les termes sont alternativement positifs et négatifs; en outre, la valeur absolue du rapport du terme de rang n au précédent est

$$\frac{n^2}{n^2+n-2}\frac{1}{x};$$

ce rapport est égal à $\frac{1}{x}$ pour $n=2$, mais il est inférieur à $\frac{1}{x}$ pour toutes les valeurs de n supérieures à 2; donc, lors même que x se réduirait à 1, les valeurs absolues des termes de la série (5) décroissent à partir du deuxième terme. Il résulte évidemment de là que l'on a

$$\log \frac{\varphi(x)}{\varphi(x+1)} < \frac{1}{12x^2},$$

ou

$$(6)\qquad \frac{\varphi(x)}{\varphi(x+1)} < e^{\frac{1}{12x^2}}.$$

Mais on peut assigner une limite de $\frac{\varphi(x)}{\varphi(x+1)}$ plus petite que la précédente, et, comme elle nous sera utile plus loin, il convient de l'indiquer ici.

Si l'on multiplie la formule (5) par $x+1$, il vient

$$(x+1)\log \frac{\varphi(x)}{\varphi(x+1)} = \frac{1}{12x} - \frac{1}{120x^3} + \ldots$$
$$+ \frac{(n-3)}{2(n-1)n(n+1)}\,\frac{(-1)^{n-1}}{x^{n-1}} + \ldots;$$

dans cette série, le terme en $\frac{1}{x^2}$ manque; les autres termes sont alternativement positifs et négatifs, et le rapport du terme en $\frac{1}{x^n}$ au terme en $\frac{1}{x^{n-1}}$ a pour valeur absolue

$$\frac{(n-1)(n-2)}{(n-1)(n-2)+2(n-4)}\,\frac{1}{x};$$

ce rapport est égal à $\frac{1}{x}$ pour $n=4$, mais il est inférieur à $\frac{1}{x}$ pour $n>4$. Donc les termes diminuent à partir du

deuxième, lors même que x serait égal à 1, et l'on a

$$(x+1)\log\frac{\varphi(x)}{\varphi(x+1)} < \frac{1}{12x},$$

ou

$$(7)\qquad \log\frac{\varphi(x)}{\varphi(x+1)} < \frac{1}{12x(x+1)}.$$

391. La formule (6) montre que l'on a

$$(8)\qquad \frac{\varphi(x)}{\varphi(x+1)} = e^{\frac{\theta_0}{x^2}},$$

θ_0 étant un nombre positif inférieur à $\frac{1}{12}$; on aura aussi, en changeant x en $x+1$, $x+2$, ..., $2x-1$, et en désignant par θ_1, θ_2, ..., θ_{x-1} des nombres compris entre zéro et $\frac{1}{12}$,

$$(9)\qquad \left\{\begin{aligned} &\frac{\varphi(x+1)}{\varphi(x+2)} = e^{\frac{\theta_1}{(x+1)^2}},\\ &\frac{\varphi(x+2)}{\varphi(x+3)} = e^{\frac{\theta_2}{(x+2)^2}}, \quad \ldots,\\ &\frac{\varphi(2x-1)}{\varphi(2x)} = e^{\frac{\theta_{x-1}}{(2x-1)^2}}. \end{aligned}\right.$$

Multiplions entre elles les égalités (8) et (9); comme la somme des x fractions

$$\frac{\theta_0}{x^2} + \frac{\theta_1}{(x+1)^2} + \frac{\theta_2}{(x+2)^2} + \ldots + \frac{\theta_{x-1}}{(2x-1)^2}$$

est moindre que $\frac{1}{12}\cdot\frac{1}{x^2}\times x$ ou que $\frac{1}{12x}$, on aura

$$(10)\qquad \frac{\varphi(x)}{\varphi(2x)} = e^{\frac{\theta}{x}},$$

θ étant un nombre compris entre zéro et $\frac{1}{12}$, et par suite

$$(11) \qquad \frac{\varphi(x)}{\varphi(2x)} = 1 \quad (\text{pour } x = \infty).$$

Si maintenant on divise la formule (1) par la formule (11), il viendra

$$(12) \qquad \varphi(x) = 1 \quad (\text{pour } x = \infty),$$

c'est-à-dire, à cause de la formule (2),

$$(13) \qquad 1.2.3\ldots x = \sqrt{2\pi}e^{-x}x^{x+\frac{1}{2}}(1+\varepsilon_x),$$

ε_x désignant une quantité positive qui s'annule pour $x = \infty$, et dont nous allons faire connaître une limite supérieure.

392. Posons, comme nous l'avons déjà fait dans la Section II de cet Ouvrage,

$$(14) \qquad \Gamma(x+1) = 1.2.3\ldots x;$$

on peut obtenir facilement, par ce qui précède, une expression complète du produit $\Gamma(x+1)$, ou, ce qui revient au même, une expression du logarithme népérien $\log\Gamma(x+1)$. On a d'abord, par la formule (2),

$$(15) \quad \log\Gamma(x+1) = \frac{1}{2}\log 2\pi - x + \left(x+\frac{1}{2}\right)\log x + \log\varphi(x),$$

et l'on a ensuite identiquement

$$\log\varphi(x) = \log\frac{\varphi(x)}{\varphi(x+1)} + \log\frac{\varphi(x+1)}{\varphi(x+2)} + \ldots$$
$$+ \log\frac{\varphi(x+m)}{\varphi(x+m+1)} + \log\varphi(x+m+1);$$

mais si l'entier m croît indéfiniment, $\varphi(x+m+1)$ tend vers l'unité, d'après la formule (12), et son loga-

rithme tend vers zéro; on a donc

$$(16) \qquad \log\varphi(x) = \sum_{m=0}^{m=\infty} \log \frac{\varphi(x+m)}{\varphi(x+m+1)};$$

ou, d'après la formule (4),

$$(17) \quad \log\varphi(x) = \sum_{m=0}^{m=\infty} \left[\left(x+m+\frac{1}{2}\right)\log\left(1+\frac{1}{x+m}\right)-1\right],$$

et l'on aura en conséquence

$$(18) \begin{cases} \log\Gamma(x+1) = \frac{1}{2}\log 2\pi - x + \left(x+\frac{1}{2}\right)\log x \\ \qquad + \sum_{m=0}^{m=\infty} \left[\left(x+m+\frac{1}{2}\right)\log\left(1+\frac{1}{x+m}\right)-1\right]. \end{cases}$$

Cette formule (18), qui a été rencontrée par Gudermann, se déduit bien facilement, comme on le voit, de la simple formule de Wallis.

393. On peut tirer la formule de Stirling de la formule (18), mais je n'entreprendrai point ici cette transformation et je me bornerai à déterminer les limites de $\log\Gamma(x+1)$ qui nous sont nécessaires.

Comme la quantité $\log\varphi(x)$ est positive, la formule (15) nous donne d'abord

$$(19) \quad \log\Gamma(x+1) > \frac{1}{2}\log 2\pi - x + \left(x+\frac{1}{2}\right)\log x.$$

Ensuite nous aurons, par la formule (16), à cause de l'inégalité (7),

$$\log\varphi(x) < \sum_{m=0}^{m=\infty} \frac{1}{12(x+m)(x+m+1)};$$

or la fraction $\frac{1}{(x+m)(x+m+1)}$ se décompose en

$$\frac{1}{x+m} - \frac{1}{x+m+1};$$

donc on peut écrire

$$12\log\varphi(x) < \left(\frac{1}{x} - \frac{1}{x+1}\right) + \left(\frac{1}{x+1} - \frac{1}{x+2}\right) + \left(\frac{1}{x+2} - \frac{1}{x+3}\right) + \cdots$$

La série contenue dans le second membre de cette formule a pour somme $\frac{1}{x}$, et l'on a en conséquence

$$\log\varphi(x) < \frac{1}{12x},$$

puis

$$(20)\quad \log\Gamma(x+1) < \frac{1}{2}\log 2\pi - x + \left(x + \frac{1}{2}\right)\log x + \frac{1}{12x}.$$

Les formules (19) et (20) nous donnent les deux limites que nous voulions trouver. En revenant des logarithmes aux nombres, on obtient

$$(21)\quad \begin{cases} 1.2.3\ldots x > \sqrt{2\pi}\, e^{-x} x^{x+\frac{1}{2}}, \\ 1.2.3\ldots x < \sqrt{2\pi}\, e^{-x+\frac{1}{12x}} x^{x+\frac{1}{2}}. \end{cases}$$

Extension des formules précédentes au cas où x n'est pas un nombre entier positif.

394. On désigne habituellement par le symbole $\Gamma(x+1)$ une certaine fonction de x qui a une valeur déterminée pour toutes les valeurs réelles et imaginaires de x, qui ne devient infinie que pour les valeurs de x égales à un

nombre entier négatif et qui se réduit au produit $1.2.3\ldots x$ quand x est un entier positif; elle coïncide, dans ce dernier cas, avec la fonction dont nous venons de nous occuper.

On arrive très-facilement à la notion des fonctions générales Γ quand on cherche à *interpoler* la fonction numérique $1.2.3\ldots x$, c'est-à-dire quand on cherche à représenter le produit $1.2.3\ldots x$ par une fonction de x qui conserve une signification bien définie lorsque x cesse de représenter un nombre entier positif.

En effet, soient x et m deux nombres entiers positifs. Les x fractions

$$\frac{m}{m+1},\quad \frac{m}{m+2},\quad \ldots,\quad \frac{m}{m+x}$$

tendront vers l'unité si, x restant constant, on fait croître m indéfiniment; il en sera donc de même du produit de ces x fractions, et l'on aura

$$\frac{m^x}{(m+1)(m+2)\ldots(m+x)}(1+\varepsilon_m)=1,$$

ε_m désignant une quantité qui s'annule pour $m=\infty$. On peut écrire aussi

$$\frac{(1.2.3\ldots m)m^x}{1.2.3\ldots(m+x)}(1+\varepsilon_m)=1$$

ou, en multipliant les deux membres par $1.2.3\ldots x$,

$$1.2.3\ldots x=\frac{(1.2.3\ldots m)m^x}{(x+1)(x+2)\ldots(x+m)}(1+\varepsilon_m).$$

Faisant tendre l'entier m vers l'infini, on aura

$$(1)\quad 1.2.3\ldots x=\lim\frac{(1.2.3\ldots m)m^x}{(x+1)(x+2)\ldots(x+m)},\quad (\text{pour } m=\infty).$$

Le second membre de cette formule devient infini

quand x est un entier négatif, mais par toutes les autres valeur réelles ou imaginaires de x il a une valeur finie et déterminée, comme on le démontre très-aisément. Si donc on pose

$$(2)\quad \Gamma(x+1)=\lim \frac{(1.2.3\ldots m)m^x}{(x+1)(x+2)\ldots(x+m)} \quad (\text{pour } m=\infty),$$

on aura, dans le cas de x entier positif,

$$\Gamma(x+1)=1.2.3\ldots x.$$

Cherchons la valeur de $\Gamma\left(\frac{1}{2}\right)$. Si l'on fait $x=-\frac{1}{2}$ dans la formule (2), il vient

$$\Gamma\left(\frac{1}{2}\right)=\frac{(1.2.3\ldots m)^2 2^{2m} m^{-\frac{1}{2}}}{1.2.3\ldots 2m} \quad (\text{pour } m=\infty),$$

et en posant, comme au n° 390,

$$\varphi(m)=\frac{1.2.3\ldots m}{\sqrt{2\pi}\,e^{-m}\,m^{m+\frac{1}{2}}},$$

on peut écrire

$$\Gamma\left(\frac{1}{2}\right)=\sqrt{\pi}\,\frac{[\varphi(m)]^2}{\varphi(2m)} \quad (\text{pour } m=\infty).$$

Enfin, comme $\varphi(m)$ et $\varphi(2m)$ se réduisent à l'unité, pour $m=\infty$, on a

$$\Gamma\left(\frac{1}{2}\right)=\sqrt{\pi}.$$

395. D'après ce qui précède, on peut écrire

$$(1)\quad \Gamma(x+1)=\frac{(1.2.3\ldots m)m^x}{(x+1)(x+2)\ldots(x+m)}(1+\varepsilon_m),$$

ε_m étant une quantité qui s'annule pour $m=\infty$. On tire

de cette formule

$$\log\Gamma(x+1) = \left[x\log\frac{2}{1} - \log\frac{x+1}{1}\right]\cdots$$
$$+\left[x\log\frac{m}{m-1} - \log\frac{x+m}{m}\right] + \log(1+\varepsilon_m),$$

ou, en écrivant $m+2$ au lieu de m et faisant tendre m vers l'infini,

$$(2)\quad \log\Gamma(x+1) = \sum_{m=0}^{m=\infty}\left[x\log\left(1+\frac{1}{m+1}\right) - \log\left(1+\frac{x}{m+1}\right)\right].$$

Cette formule (2) est équivalente à la formule (1) et elle exprime, comme celle-ci, la définition générale des fonctions Γ.

Il est facile maintenant d'établir la généralité de la formule (18) du n° 392. En effet, cette formule (18) et la formule qui précède s'accordent à donner, par une double différentiation,

$$\frac{d^2\log\Gamma(x+1)}{dx^2} = \sum_{m=0}^{m=\infty}\frac{1}{(x+m+1)^2};$$

les premiers membres de ces deux formules ayant ainsi la même dérivée du deuxième ordre, ils ne peuvent différer que par une fonction linéaire de x; mais, comme ils sont égaux pour toutes les valeurs de x entières et positives, on en conclut qu'ils sont égaux, quel que soit x.

396. Nous ne pouvons nous dispenser de rappeler ici que, si x est une quantité positive, la fonction $\Gamma(x)$ n'est autre chose que celle qui a reçu de Legendre la dénomination d'*intégrale eulérienne de seconde espèce*. Effectivement, en écrivant $x-1$ au lieu de x, la formule (1) du numéro précédent devient

$$\Gamma(x) = \frac{(1.2.3\ldots m)\,m^{x-1}}{x(x+1)\ldots(x+m-1)} \quad (\text{pour } m=\infty).$$

Intégrons par parties la différentielle $\alpha^{x-1}(1-\alpha)^m d\alpha$, il viendra

$$\int \alpha^{x-1}(1-\alpha)^m d\alpha = \frac{\alpha^x(1-\alpha)^m}{x} + \frac{m}{x}\int \alpha^x(1-\alpha)^{m-1}d\alpha;$$

et comme x est positive, si l'on prend les intégrales entre les limites zéro et 1, on aura

$$\int_0^1 \alpha^{x-1}(1-\alpha)^m d\alpha = \frac{m}{x}\int_0^1 \alpha^x(1-\alpha)^{m-1}d\alpha.$$

On conclut de là, quel que soit l'entier n,

$$\int_0^1 \alpha^{x-1}(1-\alpha)^m d\alpha = \frac{m(m-1)\ldots(m-n+1)}{x(x+1)\ldots(x+n-1)}\int_0^1 \alpha^{x+n-1}(1-\alpha)^{m-n}d\alpha;$$

pour $n=m$, l'intégrale du second membre se réduit à $\int_0^1 x^{x+m-1}d\alpha = \frac{1}{x+m}$; donc on a

$$\int_0^1 \alpha^{x-1}(1-\alpha)^m d\alpha = \frac{1.2.3\ldots m}{x(x+1)\ldots(x+m)},$$

et, en écrivant $\frac{\alpha}{m}$, $\frac{d\alpha}{m}$ au lieu de α et $d\alpha$,

$$\frac{x+m}{m}\int_0^m \alpha^{x-1}\left(1-\frac{\alpha}{m}\right)^m d\alpha = \frac{(1.2.3\ldots m)m^{x-1}}{x(x+1)\ldots(x+m-1)}.$$

On a, d'après cela

$$\Gamma(x) = \left(1+\frac{x}{m}\right)\int_0^m \alpha^{x-1}\left(1-\frac{\alpha}{m}\right)^m d\alpha \quad (\text{pour } m=\infty);$$

on peut écrire aussi

$$\Gamma(x) = \left(1+\frac{x}{m}\right)\left[\int_0^M \alpha^{x-1}\left(1-\frac{\alpha}{m}\right)^m d\alpha \right.$$
$$\left. + \int_M^m \alpha^{x-1}\left(1-\frac{\alpha}{m}\right)^m d\alpha\right] (\text{pour } m=\infty).$$

La quantité $\left(1-\frac{\alpha}{m}\right)^m$ a pour logarithme

$$-\left(\alpha+\frac{\alpha^2}{2m}+\frac{\alpha^3}{3m^2}+\ldots\right)$$

et, α étant regardée comme constante, elle atteint son maximum pour $m=\infty$; ce maximum est $e^{-\alpha}$. On a donc

$$\int_M^m \alpha^{x-1}\left(1-\frac{\alpha}{m}\right)^m d\alpha < \int_M^m \alpha^{x-1}e^{-\alpha}d\alpha,$$

et l'on pourra poser

$$\int_M^m \alpha^{x-1}\left(1-\frac{\alpha}{m}\right)^m d\alpha = (1-\theta)\int_M^m \alpha^{x-1}e^{-\alpha}d\alpha,$$

θ étant une quantité comprise entre zéro et 1. L'expression de $\Gamma(x)$ devient alors

$$\Gamma(x)=\left(1+\frac{x}{m}\right)\left[\int_0^M \alpha^{x-1}\left(1-\frac{\alpha}{m}\right)^m d\alpha \right.$$
$$\left. +(1-\theta)\int_M^m \alpha^{x-1}e^{-\alpha}d\alpha\right] \text{ (pour } m=\infty);$$

regardant maintenant M comme une constante, faisons tendre m vers l'infini, on aura à la limite $\left(1-\frac{\alpha}{m}\right)^m = e^{-\alpha}$, et par suite

$$\Gamma(x)=\int_0^\infty \alpha^{x-1}e^{-\alpha}d\alpha - \theta\int_M^\infty \alpha^{x-1}e^{-\alpha}d\alpha;$$

mais il est évident que la quantité θ est ici rigoureusement nulle, car la formule précédente a lieu, quel que soit M, et la dernière partie disparaît pour $M=\infty$. On a donc

$$\Gamma(x)=\int_0^\infty \alpha^{x-1}e^{-\alpha}d\alpha,$$

pour toutes les valeurs positives de x.

Détermination de deux limites entre lesquelles reste comprise la somme des logarithmes népériens de tous les entiers qui ne surpassent pas un nombre donné.

397. Soit a un nombre entier positif; faisons $x = a+1$ dans la formule (19) du n° 393 et retranchons ensuite $\log(a+1)$ de chaque membre; faisons en même temps $x = a$ dans la formule (20) du même numéro, on aura

$$(1)\quad \left\{\begin{aligned} &\log 1.2.3\ldots a > \log\sqrt{2\pi} + (a+1)\log(a+1) - (a+1) - \frac{1}{2}\log(a+1),\\ &\log 1.2.3\ldots a < \log\sqrt{2\pi} + a\log a - a + \frac{1}{2}\log a + \frac{1}{12a}.\end{aligned}\right.$$

Cela posé, désignons par x une quantité positive quelconque au moins égale à 1, et soit a le plus grand entier contenu dans x. On a, par hypothèse,

$$a \leqq x < a+1 \quad \text{et} \quad a \geqq 1,$$

et l'on en déduit

$$\left(a+1-\frac{1}{2}\right)[\log(a+1)-1] > \left(x-\frac{1}{2}\right)(\log x - 1),$$

$$\left(a+\frac{1}{2}\right)(\log a - 1) + \frac{1}{12a} \mathrel{\substack{=\\<}} \left(x+\frac{1}{2}\right)(\log x - 1) + \frac{1}{12},$$

ou

$$(2)\quad \left\{\begin{aligned} &(a+1)\log(a+1) - (a+1) - \frac{1}{2}\log(a+1)\\ &\qquad > x\log x - x - \frac{1}{2}\log x,\\ &a\log a - a + \frac{1}{2}\log a + \frac{1}{12a}\\ &\qquad \mathrel{\substack{=\\<}} x\log x - x + \frac{1}{2}\log x + \frac{1}{12}.\end{aligned}\right.$$

Des inégalités (1) et (2) on conclut, en appelant $T(x)$ le

logarithme du produit de tous les nombres entiers qui ne surpassent pas x,

$$(3)\quad \begin{cases} T(x) > \log\sqrt{2\pi} + x\log x - x - \dfrac{1}{2}\log x, \\ T(x) < \log\sqrt{2\pi} + x\log x - x + \dfrac{1}{2}\log x + \dfrac{1}{12}. \end{cases}$$

Ces inégalités (3) sont celles que nous voulions obtenir.

Sur la totalité des nombres premiers compris entre deux limites données.

398. Le problème qui consiste à déterminer combien il y a de nombres premiers compris entre deux nombres donnés n'a pas encore été résolu et semble présenter les plus grandes difficultés. M. Tchébichef est le premier qui se soit occupé avec succès de cette question; dans un Mémoire présenté en 1850 à l'Académie impériale des Sciences de Saint-Pétersbourg, cet habile géomètre a donné le moyen d'assigner deux limites entre lesquelles est nécessairement compris le nombre qui exprime combien il y a de nombres premiers entre deux nombres donnés. M. Tchébichef a déduit de son analyse la démonstration d'un *postulatum* sur lequel M. Bertrand avait fondé la démonstration d'un théorème important dont il sera question dans la Section suivante. Ce *postulatum* consiste en ce que :

Il y a toujours au moins un nombre premier compris entre a et $2a - 2$ si a est supérieur à $\frac{7}{2}$.

Bien que je sois parvenu à démontrer le théorème dont il s'agit sans recourir à aucun *postulatum*, ainsi qu'on le verra dans la Section IV, je ne crois pas inutile de pré-

senter ici l'analyse ingénieuse de M. Tchébichef, analyse qui repose sur des considérations entièrement neuves.

Nous désignerons par $T(z)$, comme au numéro précédent, la somme des logarithmes népériens de tous les nombres entiers qui ne surpassent pas z ; nous désignerons en outre par $\theta(z)$ la somme des logarithmes népériens de tous les nombres *premiers* qui ne surpassent pas z. Les fonctions $T(z)$ et $\theta(z)$ se réduisent à zéro lorsque z est inférieur à 2. Quand z sera une quantité composée, comme $\left(\frac{x}{2}\right)^{\frac{1}{2}}$ par exemple, nous écrirons, pour abréger, $\theta\left(\frac{x}{2}\right)^{\frac{1}{2}}$ au lieu de $\theta\left[\left(\frac{x}{2}\right)^{\frac{1}{2}}\right]$.

Propriété fondamentale de la fonction $\theta(z)$.

399. La propriété fondamentale sur laquelle reposent les recherches de M. Tchébichef consiste dans l'égalité suivante :

$$\begin{aligned} T(x) = {} & \theta(x) + \theta(x)^{\frac{1}{2}} + \theta(x)^{\frac{1}{3}} + \theta(x)^{\frac{1}{4}} + \ldots \\ & + \theta\left(\frac{x}{2}\right) + \theta\left(\frac{x}{2}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{2}\right)^{\frac{1}{3}} + \theta\left(\frac{x}{2}\right)^{\frac{1}{4}} + \ldots \\ & + \theta\left(\frac{x}{3}\right) + \theta\left(\frac{x}{3}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{3}\right)^{\frac{1}{3}} + \theta\left(\frac{x}{3}\right)^{\frac{1}{4}} + \ldots \\ & + \theta\left(\frac{x}{4}\right) + \theta\left(\frac{x}{4}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{4}\right)^{\frac{1}{3}} + \theta\left(\frac{x}{4}\right)^{\frac{1}{4}} + \ldots \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{aligned}$$

où les séries doivent être prolongées jusqu'aux termes qui deviennent zéro.

Pour démontrer cette égalité, remarquons que chaque membre est égal à une somme de termes tels que $k \log \alpha$,

k désignant un entier et α un nombre premier. Supposons que, dans la suite des nombres 1, 2, 3, 4, ..., qui ne surpassent pas x, il y en ait A_1 qui soient divisibles par α; nommons aussi A_2 le nombre de ceux qui sont divisibles par α^2, et généralement A_i le nombre de ceux qui sont divisibles par α^i; il est clair que le coefficient de $\log\alpha$ dans $T(x)$ sera $A_1 + A_2 + A_3 + \ldots.$ Considérons maintenant les termes qui composent une ligne verticale du second membre de notre égalité, par exemple,

$$\theta(x)^{\frac{1}{i}},\quad \theta\left(\frac{x}{2}\right)^{\frac{1}{i}},\quad \theta\left(\frac{x}{3}\right)^{\frac{1}{i}},\quad \theta\left(\frac{x}{4}\right)^{\frac{1}{i}},\quad \ldots;$$

on trouvera, dans cette suite, autant de termes contenant $\log\alpha$ avec le coefficient 1 qu'il y a de quantités qui ne sont pas inférieures à α dans la suite

$$x^{\frac{1}{i}},\quad \left(\frac{x}{2}\right)^{\frac{1}{i}},\quad \left(\frac{x}{3}\right)^{\frac{1}{i}},\quad \left(\frac{x}{4}\right)^{\frac{1}{i}},\quad \ldots.$$

Or le nombre de ces quantités est évidemment le même que le nombre des quantités

$$\alpha^i,\quad 2\alpha^i,\quad 3\alpha^i,\quad 4\alpha^i,\quad \ldots,$$

qui ne surpassent pas x; ce nombre est précisément celui que nous avons désigné par A_i. Donc le coefficient de $\log\alpha$ dans le deuxième membre de notre égalité est $A_1 + A_2 + A_3 + \ldots$, ce qui démontre l'exactitude de cette égalité.

Nous ferons, pour abréger,

$$(1)\qquad \psi(z) = \theta(z) + \theta(z)^{\frac{1}{2}} + \theta(z)^{\frac{1}{3}} + \theta(z)^{\frac{1}{4}} + \ldots,$$

et alors l'égalité que nous venons d'établir pourra s'écrire ainsi :

$$(2)\qquad T(x) = \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \psi\left(\frac{x}{4}\right) + \ldots.$$

Démonstration de deux inégalités auxquelles satisfait la fonction $\psi(z)$.

400. Les deux inégalités que nous proposons d'établir sont les suivantes :

$$\psi(x) > T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right),$$

$$\psi(x) - \psi\left(\frac{x}{6}\right) < T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right).$$

L'équation (2) du n° 399 donne

$$(1)\quad \left\{\begin{aligned} & T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ &= \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \psi\left(\frac{x}{4}\right) + \ldots \\ &+ \psi\left(\frac{x}{30}\right) + \psi\left(\frac{x}{2.30}\right) + \psi\left(\frac{x}{3.30}\right) + \psi\left(\frac{x}{4.30}\right) + \ldots \\ &- \psi\left(\frac{x}{2}\right) - \psi\left(\frac{x}{2.2}\right) - \psi\left(\frac{x}{3.2}\right) - \psi\left(\frac{x}{4.2}\right) - \ldots \\ &- \psi\left(\frac{x}{3}\right) - \psi\left(\frac{x}{2.3}\right) - \psi\left(\frac{x}{3.3}\right) - \psi\left(\frac{x}{4.3}\right) - \ldots \\ &- \psi\left(\frac{x}{5}\right) - \psi\left(\frac{x}{2.5}\right) - \psi\left(\frac{x}{3.5}\right) - \psi\left(\frac{x}{4.5}\right) - \ldots . \end{aligned}\right.$$

Le second membre de cette équation est de la forme

$$A_1\psi(x) + A_2\,\psi\left(\frac{x}{2}\right) + A_3\,\psi\left(\frac{x}{3}\right) + \ldots + A_n\,\psi\left(\frac{x}{n}\right) + \ldots,$$

A_1, A_2, A_3, ... étant des coefficients entiers. Or je dis qu'on a en général :

$A_n = 1$, si n n'est divisible par aucun des facteurs 2, 3, 5;
$A_n = 0$, si n est divisible par un seul des facteurs 2, 3, 5;
$A_n = -1$, si n est divisible par deux au moins des facteurs 2, 3, 5;
$A_n = -1$, si n est divisible par chacun des facteurs 2, 3, 5.

En effet, dans le premier cas, où n n'est divisible par aucun des nombres 2, 3, 5, on ne trouve le terme $\psi\left(\frac{x}{n}\right)$ que dans la première ligne horizontale du second membre de l'équation (1). Dans le deuxième cas, où n est divisible par un seul des nombres 2, 3, 5, on trouvera le terme $\psi\left(\frac{x}{n}\right)$ avec le signe — dans une quelconque des trois dernières lignes horizontales du second membre de l'équation (1), et comme ce terme existe dans la première ligne avec le signe +, on trouvera zéro, après la réduction, pour coefficient de $\psi\left(\frac{x}{n}\right)$. Dans le troisième cas, où n est divisible par deux des nombres 2, 3, 5, le terme $\psi\left(\frac{x}{n}\right)$ se trouve avec le signe + dans la première ligne horizontale du second membre de l'équation (1), et avec le signe — dans deux des trois dernières lignes ; donc il ne restera après la réduction que $-\psi\left(\frac{x}{n}\right)$. Enfin, dans le quatrième cas, où n est divisible par chacun des nombres 2, 3, 5, le terme $\psi\left(\frac{x}{n}\right)$ se trouve avec le signe + dans les deux premières lignes du second membre de l'équation (1), et avec le signe — dans les trois dernières lignes ; il restera donc encore $-\psi\left(\frac{x}{n}\right)$ après la réduction. Donc, pour

$n = 30m +$	1,	2,	3,	4,	5,	6,	7,	8,	9,	10,
	11,	12,	13,	14,	15,	16,	17,	18,	19,	20,
	21,	22,	23,	24,	25,	26,	27,	28,	29,	30.

on a

$A_n =$	1,	0,	0,	0,	0,	-1,	1,	0,	0,	-1,
	1,	-1,	1,	0,	-1,	0,	1,	-1,	1,	-1,
	0,	0,	1,	-1,	0,	0,	0,	0,	1,	-1,

et, par conséquent, l'équation (1) se réduit à

$$T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)$$

$$= \psi(x) - \psi\left(\frac{x}{6}\right) + \psi\left(\frac{x}{7}\right) - \psi\left(\frac{x}{10}\right) + \psi\left(\frac{x}{11}\right) - \psi\left(\frac{x}{12}\right) + \ldots,$$

où tous les termes du second membre ont pour coefficient $+1$ et -1 alternativement. Or la fonction $\psi(z)$ ne peut croître quand z décroît; donc la série

$$\psi(x) - \psi\left(\frac{x}{6}\right) + \psi\left(\frac{x}{7}\right) - \psi\left(\frac{x}{10}\right) + \ldots,$$

qui forme le second membre de l'équation précédente, est comprise entre

$$\psi(x) \quad \text{et} \quad \psi(x) - \psi\left(\frac{x}{6}\right);$$

on a donc

$$(2) \quad \begin{cases} \psi(x) \geqq T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ \psi(x) - \psi\left(\frac{x}{6}\right) \leqq T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right); \end{cases}$$

ce qu'il fallait démontrer.

Détermination de deux limites entre lesquelles sont comprises les fonctions $\psi(z)$ et $\theta(z)$.

401. On a vu, au n° 397, que la fonction $T(x)$ satisfait aux deux inégalités

$$(1) \quad \begin{cases} T(x) < \log\sqrt{2\pi} + x\log x - x + \frac{1}{2}\log x + \frac{1}{12}, \\ T(x) > \log\sqrt{2\pi} + x\log x - x - \frac{1}{2}\log x. \end{cases}$$

On déduit de là

$$T(x)+T\left(\frac{x}{30}\right)<2\log\sqrt{2\pi}+\frac{2}{12}$$
$$+\frac{31}{30}x\log x-x\log 30^{\frac{1}{30}}-\frac{31}{30}x+\log x-\frac{1}{2}\log 30,$$

$$T(x)+T\left(\frac{x}{30}\right)>2\log\sqrt{2\pi}$$
$$+\frac{31}{30}x\log x-x\log 30^{\frac{1}{30}}-\frac{31}{30}x-\log x+\frac{1}{2}\log 30,$$

et

$$T\left(\frac{x}{2}\right)+T\left(\frac{x}{3}\right)+T\left(\frac{x}{5}\right)<3\log\sqrt{2\pi}+\frac{3}{12}$$
$$+\frac{31}{30}x\log x-x\log 2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}-\frac{31}{30}x+\frac{3}{2}\log x-\frac{1}{2}\log 30,$$

$$T\left(\frac{x}{2}\right)+T\left(\frac{x}{3}\right)+T\left(\frac{x}{5}\right)>3\log\sqrt{2\pi}$$
$$+\frac{31}{30}x\log x-x\log 2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}-\frac{31}{30}x-\frac{3}{2}\log x+\frac{1}{2}\log 30.$$

Retranchant la quatrième de ces inégalités de la première, et la troisième de la deuxième, il vient

$$T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)$$
$$<x\log\frac{2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}}{30^{\frac{1}{30}}}+\frac{5}{2}\log x-\frac{1}{2}\log 1800\pi+\frac{2}{12},$$

$$T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)$$
$$>x\log\frac{2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}}{30^{\frac{1}{30}}}-\frac{5}{2}\log x+\frac{1}{2}\log\frac{450}{\pi}-\frac{3}{12}.$$

Nous ferons, pour abréger,

$$A = \log \frac{2^{\frac{1}{2}} 3^{\frac{1}{3}} 5^{\frac{1}{5}}}{30^{\frac{1}{30}}} = 0,92129202\ldots;$$

alors les inégalités précédentes deviendront

$$(2)\quad \left\{\begin{aligned} &T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ &\qquad < Ax + \frac{5}{2}\log x - \frac{1}{2}\log 1800\pi + \frac{2}{12}, \\ &T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \\ &\qquad > Ax - \frac{5}{2}\log x + \frac{1}{2}\log\frac{450}{\pi} - \frac{3}{12}, \end{aligned}\right.$$

et l'on voit que l'on a, à plus forte raison,

$$(3)\quad \left\{\begin{aligned} &T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) < Ax + \frac{5}{2}\log x, \\ &T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) > Ax - \frac{5}{2}\log x - 1. \end{aligned}\right.$$

Les formules (1) n'ont lieu que dans l'hypothèse de $x > 1$; d'ailleurs, pour former les inégalités (2), on a remplacé x par $\frac{x}{2}, \frac{x}{3}, \frac{x}{5}, \frac{x}{30}$; donc les formules (2) ne sont établies que dans l'hypothèse de $x > 30$. Mais il est facile de vérifier que les formules (3) ont lieu pour toutes les valeurs de x comprises entre 1 et 30, et, par suite, qu'elles ne présentent aucune exception.

Des inégalités (3), combinées avec les inégalités (2) du n° **400**, on déduit

$$(4)\quad \left\{\begin{aligned} &\psi(x) > Ax - \frac{5}{2}\log x - 1, \\ &\psi(x) - \psi\left(\frac{x}{6}\right) < Ax + \frac{5}{2}\log x. \end{aligned}\right.$$

La première de ces formules donne immédiatement une limite inférieure de $\psi(x)$; la seconde peut servir, comme on va le voir, à obtenir une limite supérieure. Pour cela, posons

$$f(x) = \frac{6}{5}\,Ax + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x,$$

on aura

$$f\left(\frac{x}{6}\right) = \frac{1}{5}\,Ax + \frac{5}{4\log 6}\log^2 x - \frac{5}{4}\log x,$$

et, par suite,

$$f(x) - f\left(\frac{x}{6}\right) = Ax + \frac{5}{2}\log x;$$

on a donc

$$\psi(x) - \psi\left(\frac{x}{6}\right) < f(x) - f\left(\frac{x}{6}\right)$$

ou bien

$$\psi(x) - f(x) < \psi\left(\frac{x}{6}\right) - f\left(\frac{x}{6}\right);$$

en changeant successivement x en $\frac{x}{6}, \frac{x}{6^2}, \frac{x}{6^3}, \ldots, \frac{x}{6^{m+1}}$, il vient

$$(5)\quad \left\{\begin{array}{l} \psi(x) - f(x) < \psi\left(\frac{x}{6}\right) - f\left(\frac{x}{6}\right) < \psi\left(\frac{x}{6^2}\right) - f\left(\frac{x}{6^2}\right) < \ldots \\ \qquad < \psi\left(\frac{x}{6^{m+1}}\right) - f\left(\frac{x}{6^{m+1}}\right). \end{array}\right.$$

Supposons maintenant que m soit le plus grand entier qui vérifie la condition $6^m \leqq x$; $\frac{x}{6^{m+1}}$ tombera entre 1 et $\frac{1}{6}$, et, par suite, $\psi\left(\frac{x}{6^{m+1}}\right)$ sera zéro ; je dis en outre que $-f\left(\frac{x}{6^{m+1}}\right)$ sera moindre que 1. En effet, la valeur de

$-f(z)$ peut s'écrire ainsi :

$$-f(z) = \frac{5\log 6}{16} - \frac{5}{4\log 6}\left(\log z + \frac{1}{2}\log 6\right)^2 - \frac{6}{5}\,\mathrm{A}z;$$

d'où l'on conclut

$$-f(z) < \frac{5\log 6}{16},$$

et, à plus forte raison,

$$-f(z) < 1,$$

puisque, 6 étant moindre que e^3, $\log 6$ est inférieur à 3.

D'après cela, la formule (5) donne

$$\psi(x) - f(x) < 1,$$

et, par suite,

$$(6) \qquad \psi(x) < \frac{6}{5}\,\mathrm{A}x + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x + 1.$$

Les deux limites que nous venons de trouver pour la fonction $\psi(x)$ vont nous permettre de trouver également deux limites de la fonction $\theta(x)$.

Pour cela remarquons que la formule

$$\psi(z) = \theta(z) + \theta(z)^{\frac{1}{2}} + \theta(z)^{\frac{1}{3}} + \ldots$$

donne

$$\psi(x) - \psi(\sqrt{x}) = \theta(x) + \theta(x)^{\frac{1}{3}} + \theta(x)^{\frac{1}{5}} + \theta(x)^{\frac{1}{7}} + \ldots,$$

$$\psi(x) - 2\psi(\sqrt{x}) = \theta(x) - \left[\theta(x)^{\frac{1}{2}} - \theta(x)^{\frac{1}{3}}\right] - \left[\theta(x)^{\frac{1}{4}} - \theta(x)^{\frac{1}{5}}\right] - \ldots$$

Or la fonction $\theta(z)$ est positive ou nulle, et d'ailleurs elle ne peut croître quand z décroît; donc on a

$$(7) \qquad \begin{cases} \theta(x) \leqq \psi(x) - \psi(\sqrt{x}), \\ \theta(x) \geqq \psi(x) - 2\psi(\sqrt{x}). \end{cases}$$

Mais on vient de trouver

$$(8)\quad \begin{cases} \psi(x) < \frac{6}{5}Ax + \frac{5}{4\log 6}\log^2 x + \frac{5}{4}\log x + 1, \\ \psi(x) > Ax - \frac{5}{2}\log x - 1, \end{cases}$$

et l'on en tire

$$(9)\quad \begin{cases} \psi(\sqrt{x}) < \frac{6}{5}Ax^{\frac{1}{2}} + \frac{5}{16\log 6}\log^2 x + \frac{5}{8}\log x + 1, \\ \psi(\sqrt{x}) > Ax^{\frac{1}{2}} - \frac{5}{4}\log x - 1; \end{cases}$$

donc on a, par les inégalités (7),

$$(10)\quad \begin{cases} \theta(x) < \frac{6}{5}Ax - Ax^{\frac{1}{2}} + \frac{5}{4\log 6}\log^2 x + \frac{5}{2}\log x + 2, \\ \theta(x) > Ax - \frac{12}{5}Ax^{\frac{1}{2}} - \frac{5}{8\log 6}\log^2 x - \frac{15}{4}\log x - 3. \end{cases}$$

Ainsi la somme des logarithmes de tous les nombres premiers qui ne surpassent pas x est comprise entre les limites

$$\frac{6}{5}Ax - Ax^{\frac{1}{2}} + \frac{5}{4\log 6}\log^2 x + \frac{5}{2}\log x + 2,$$

$$Ax - \frac{12}{5}Ax^{\frac{1}{2}} - \frac{5}{8\log 6}\log^2 x - \frac{15}{4}\log x - 3.$$

Détermination de deux limites du nombre qui indique combien il y a de nombres premiers compris entre deux nombres donnés.

402. Soit m le nombre qui indique combien il y a de nombres premiers plus grands qu'un nombre donné l et qui ne surpassent pas un autre nombre donné L. La somme des logarithmes népériens de ces m nombres pre-

miers sera évidemment comprise entre $m\log l$ et $m\log L$; on aura donc

$$\theta(L) - \theta(l) > m\log l,$$
$$\theta(L) - \theta(l) < m\log L,$$

et, par conséquent,

$$m < \frac{\theta(L) - \theta(l)}{\log l}, \quad m > \frac{\theta(L) - \theta(l)}{\log L};$$

mais, d'après les inégalités (10) du n° 401, on a

$$\theta(L) - \theta(l) < A\left(\frac{6}{5}L - l\right) - A\left(L^{\frac{1}{2}} - \frac{12}{5}l^{\frac{1}{2}}\right)$$
$$+ \frac{5}{8\log 6}(2\log^2 L + \log^2 l) + \frac{5}{4}(2\log L + 3\log l) + 5,$$
$$\theta(L) - \theta(l) > A\left(L - \frac{6}{5}l\right) - A\left(\frac{12}{5}L^{\frac{1}{2}} - l^{\frac{1}{2}}\right)$$
$$- \frac{5}{8\log 6}(\log^2 L + 2\log^2 l) - \frac{5}{4}(3\log L + 2\log l) - 5;$$

donc

$$m < \frac{A\left(\frac{6}{5}L - l\right) - A\left(L^{\frac{1}{2}} - \frac{12}{5}l^{\frac{1}{2}}\right) + \frac{5}{8\log 6}(2\log^2 L + \log^2 l) + \frac{5}{4}(2\log L + 3\log l) + 5}{\log l},$$

$$m > \frac{A\left(L - \frac{6}{5}l\right) - A\left(\frac{12}{5}L^{\frac{1}{2}} - l^{\frac{1}{2}}\right) - \frac{5}{8\log 6}(\log^2 L + 2\log^2 l) - \frac{5}{4}(3\log L + 2\log l) - 5}{\log L}.$$

Ces formules donnent ainsi deux limites entre lesquelles tombe la quantité m qui désigne combien il y a de nombres premiers plus grands que l et qui ne surpassent pas L. La deuxième de ces formules montre qu'on trouvera plus de k nombres premiers entre les limites l et L, si la condition suivante est satisfaite, savoir :

$$< \frac{A\left(L - \frac{6}{5}l\right) - A\left(\frac{12}{5}L^{\frac{1}{2}} - l^{\frac{1}{2}}\right) - \frac{5}{8\log 6}(\log^2 L + 2\log^2 l) - \frac{5}{4}(3\log L + 2\log l) - 5}{\log L}$$

et, comme l est > 0 et $< L$, on vérifie cette inégalité en faisant

$$k = \frac{A\left(L - \frac{6}{5}l\right) - \frac{12}{5}AL^{\frac{1}{2}} - \frac{15}{8\log 6}\log^2 L - \frac{25}{4}\log L - 5}{\log L},$$

d'où l'on tire

$$l = \frac{5}{6}L - 2L^{\frac{1}{2}} - \frac{25}{16A\log 6}\log^2 L - \frac{5}{6A}\left(\frac{25}{4} + k\right)\log L - \frac{25}{6A}.$$

Ainsi, en prenant pour l cette valeur, on est sûr de trouver plus de k nombres premiers entre l et L. Il est bien entendu que l et L sont supposés plus grands que 1.

En faisant $k = 0$, on conclut de ce qui précède qu'il y a au moins un nombre premier entre l et L, si l'on prend

$$(3) \qquad l = \frac{5}{6}L - 2L^{\frac{1}{2}} - \frac{25\log^2 L}{16A\log 6} - \frac{125\log L}{24A} - \frac{25}{6A}.$$

Application des résultats qui précèdent.

403. Des résultats que nous venons d'obtenir il est aisé de déduire la démonstration de la proposition dont nous avons parlé au n° 398. Effectivement, nous venons de voir qu'il y a au moins un nombre premier entre les limites

$$\frac{5}{6}L - 2L^{\frac{1}{2}} - \frac{25\log^2 L}{16A\log 6} - \frac{125\log L}{24A} - \frac{25}{6A} \quad \text{et} \quad L;$$

donc il sera établi qu'il y a au moins un nombre premier entre les limites a et $2a - 2$, si l'on prouve qu'on peut, par une valeur convenable de L, satisfaire aux deux inégalités

$$2a - 2 > L,$$

$$a < \frac{5}{6}L - 2L^{\frac{1}{2}} - \frac{25\log^2 L}{16A\log 6} - \frac{125\log L}{24A} - \frac{25}{6A}.$$

Or on vérifie évidemment la première de ces inégalités en prenant

$$L = 2a - 3.$$

Quant à la seconde, elle devient, pour $L = 2a - 3$,

$$a < \frac{5}{6}(2a-3) - 2\sqrt{2a-3} - \frac{25\log^2(2a-3)}{16A\log 6} - \frac{125\log(2a-3)}{24A} - \frac{25}{6A},$$

ce qui est exact pour toutes les valeurs de a qui surpassent la plus grande racine de l'équation

$$x = \frac{5}{6}(2x-3) - 2\sqrt{2x-3} - \frac{25\log^2(2x-3)}{16A\log 6} - \frac{125\log(2x-3)}{24A} - \frac{25}{6A};$$

or on trouve que cette plus grande racine est comprise entre 159 et 160; donc, si a est > 160, il y a nécessairement un nombre premier compris entre a et $2a-2$. A l'égard des valeurs de a inférieures à 160, la proposition peut se vérifier immédiatement au moyen des Tables de nombres premiers.

SECTION IV.

LES SUBSTITUTIONS.

SECTION IV.

LES SUBSTITUTIONS.

CHAPITRE PREMIER.

PROPRIÉTÉS GÉNÉRALES DES SUBSTITUTIONS.

Des permutations formées avec des lettres données, et des substitutions par lesquelles on passe d'une permutation à une autre.

404. Les *permutations* de n lettres

$$a,\ b,\ c,\ d,\ \ldots,\ k,\ l$$

sont les résultats que l'on obtient en écrivant ces lettres à la suite les unes des autres de toutes les manières possibles, et l'on démontre dans les éléments d'Algèbre que le nombre total N de ces permutations est

$$N = 1.2.3\ldots n.$$

Représentons par de simples lettres

$$A_0.\ A_1,\ A_2,\ \ldots,\ A_{N-1}$$

les N permutations dont il s'agit. L'opération par laquelle on passe d'une permutation à une autre est dite une *substitution* (n° 235). Nous représenterons une substitution en écrivant entre parenthèses la permutation de laquelle on part, et, au-dessus de celle-ci, la permutation

nouvelle qui doit la remplacer. Ainsi le symbole

$$\begin{pmatrix} A_1 \\ A_0 \end{pmatrix}$$

désignera la substitution qui a pour effet de remplacer les lettres de la permutation A_0 par celles qui occupent respectivement les mêmes rangs dans la permutation A_1; les permutations A_0 et A_1 seront dites les *termes* de la substitution, A_0 sera le *dénominateur* et A_1 le *numérateur*. Il est évident que l'on peut choisir pour dénominateur d'une substitution donnée l'une quelconque des N permutations.

D'après cela, si l'on adopte A_0 pour dénominateur, on obtiendra toutes les substitutions en prenant successivement pour numérateurs les N permutations; ces substitutions seront donc

$$\begin{pmatrix} A_0 \\ A_0 \end{pmatrix}, \quad \begin{pmatrix} A_1 \\ A_0 \end{pmatrix}, \quad \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}, \quad \ldots, \quad \begin{pmatrix} A_{N-1} \\ A_0 \end{pmatrix}.$$

Le symbole $\begin{pmatrix} A_0 \\ A_0 \end{pmatrix}$ représente ce qu'on appelle une *substitution identique*, il indique la conservation de l'ordre des lettres; il y a avantage à le comprendre parmi les substitutions, et le nombre de celles-ci sera dès lors égal à N.

Nous représenterons souvent par de simples lettres S, T, . . . les diverses substitutions que nous aurons à considérer.

Lorsqu'une lettre occupe la même place dans le numérateur et dans le dénominateur d'une substitution, on peut la supprimer sans inconvénient. Ainsi la substitution

$$S = \begin{pmatrix} dbca\ldots \\ abcd\ldots \end{pmatrix}$$

peut s'écrire plus simplement

$$S = \begin{pmatrix} da\ldots \\ ad\ldots \end{pmatrix}.$$

On dit qu'une substitution est réduite à sa plus simple expression quand on a supprimé dans ses deux termes toutes les lettres qui y occupaient les mêmes places.

Des produits de substitutions.

405. On nomme *produit* d'une permutation donnée par une substitution la permutation nouvelle que l'on obtient en appliquant la substitution à la permutation donnée. Ce produit se représente en écrivant la substitution à gauche de la permutation donnée. Considérons, par exemple, la substitution

$$S = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix};$$

si on l'applique à la permutation A_0, on produira la permutation A_1, et nous écrirons en conséquence

$$SA_0 = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} A_0 = A_1.$$

On nomme *produit* de deux substitutions données la substitution nouvelle qui produit le même effet que les substitutions données appliquées l'une après l'autre à une permutation quelconque. Ce produit se représente en écrivant la substitution qui doit être effectuée la première à droite de l'autre substitution. Ainsi le produit de la substitution $S = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix}$ par la substitution $T = \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}$ s'écrira

$$TS \quad \text{ou} \quad \begin{pmatrix} A_2 \\ A_0 \end{pmatrix} \begin{pmatrix} A_1 \\ A_0 \end{pmatrix};$$

pareillement le produit de la substitution T par la substitution S s'écrira

$$\text{ST} \quad \text{ou} \quad \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}.$$

Si les deux produits ST et TS sont égaux, les substitutions S et T sont dites *échangeables entre elles*. Il est évident que deux substitutions qui, réduites à leur plus simple expression, n'ont aucune lettre commune, sont échangeables entre elles.

Le produit d'un nombre quelconque de substitutions S, T, U, V, ... est le résultat que l'on obtient en multipliant la première substitution par la deuxième, puis le produit obtenu par la troisième substitution, et ainsi de suite; il sera représenté par ...VUTS.

Si les substitutions qu'il s'agit de multiplier entre elles sont toutes égales à S, et que leur nombre soit égal à ν, le produit est dit la puissance $\nu^{\text{ième}}$ de S; celle-ci se représente par S^ν.

Lorsqu'une substitution identique, telle que $\begin{pmatrix} A_0 \\ A_0 \end{pmatrix}$, figure dans un produit, elle peut être supprimée, et en conséquence il est naturel de la regarder comme égale à l'unité; ainsi nous écrirons

$$\begin{pmatrix} A_0 \\ A_0 \end{pmatrix} = 1.$$

En outre, si l'on convient de regarder comme égal à l'unité le symbole S^ν, quand ν se réduit à zéro, quelle que soit la substitution S, il en résultera que la puissance zéro d'une substitution quelconque désignera une substitution identique.

Ordre d'une substitution.

406. Soit S une substitution quelconque, la série des puissances de S, en partant de S^0 ou 1, sera

$$1,\ S,\ S^2,\ S^3,\ \ldots,\ S^\nu,\ \ldots,$$

et, comme le nombre total des substitutions est limité, si l'on prolonge suffisamment la précédente suite, on verra nécessairement se reproduire des substitutions déjà obtenues. Supposons que l'on ait

$$S^{\mu+\nu} = S^\mu;$$

comme le premier membre de cette égalité est égal à $S^\nu . S^\mu$, on peut écrire

$$S^\nu S^\mu = S^\mu,$$

d'où il suit que la substitution S^ν, appliquée à une permutation quelconque, ne produira aucun déplacement des lettres; en d'autres termes, cette substitution est identique et l'on a

$$S^\nu = 1.$$

On conclut de cette égalité, quel que soit l'entier q,

$$(S^\nu)^q \quad \text{ou} \quad S^{\nu q} = 1,$$

et, en multipliant par la puissance $r^{\text{ième}}$ de S,

$$S^{\nu q + r} = S^r.$$

Il résulte de là que la série des puissances de S est périodique, et que la période se compose des substitutions

$$1,\ S,\ S^2,\ \ldots,\ S^{\nu-1}.$$

Si l'on suppose que ν soit le plus petit nombre tel que

$S^\nu = 1$, les termes de la suite précédente seront effectivement distincts; car l'égalité $S^{\mu'+\nu'} = S^{\mu'}$ entraînerait $S^{\nu'} = 1$, ce qui n'a pas lieu, puisque ν' est inférieur à ν.

On nomme *ordre* d'une substitution S le plus petit des exposants ν tels que l'on ait $S^\nu = 1$. En d'autres termes, l'ordre d'une substitution est le nombre de fois qu'il faut appliquer successivement la substitution à une permutation pour reproduire cette permutation. On voit que les seules puissances de S qui se réduisent à l'unité sont S^ν, $S^{2\nu}$, $S^{3\nu}$, ...

Nous conviendrons d'étendre l'égalité $S^{\nu q+r} = S^r$ aux valeurs négatives de r; changeons donc r en $-r$, on aura

$$S^{\nu q-r} = S^{-r},$$

et cette formule définit ce que nous appelons *puissances négatives* d'une substitution S, le nombre q étant choisi de manière que $\nu q - r$ soit positif. Si, en particulier, on pose $r = 1$, on pourra prendre $q = 1$, et l'on aura

$$S^{\nu-1} = S^{-1}.$$

Les substitutions S et S^{-1} ont pour produit l'unité; elles sont dites *inverses* l'une de l'autre. Si l'on a

$$S = \binom{A_1}{A_0},$$

on aura évidemment

$$S^{-1} = \binom{A_0}{A_1}.$$

Si une substitution S est d'ordre ν, la puissance $\mu^{\text{ième}}$ de S sera de l'ordre $\frac{\nu}{\theta}$, θ désignant le plus grand commun diviseur des nombres μ et ν. En effet, pour que l'on ait

$(S^\mu)^x = 1$ ou $S^{\mu x} = 1$, il faut que μx soit divisible par ν, ou x par $\frac{\nu}{\theta}$; d'ailleurs, cette égalité a lieu en prenant $x = \frac{\nu}{\theta}$. Donc le quotient $\frac{\nu}{\theta}$ représente l'ordre de S^μ.

On voit en particulier que si μ est premier à ν, S^μ sera de l'ordre ν. Dans ce cas, si l'on pose

$$S^\mu = T,$$

la substitution S fera partie de la suite des puissances de T. En effet, si l'on élève à la puissance x l'égalité précédente, on aura

$$S^{\mu x} = T^x \quad \text{ou} \quad S^{\mu x - \nu y} = T^x,$$

y désignant un entier quelconque. Mais ν et μ étant premiers entre eux, on peut faire en sorte que les entiers x et y satisfassent à l'équation $\mu x - \nu y = 1$, et l'on aura alors

$$S = T^x.$$

Des substitutions circulaires.

407. Soit

$$A_0 = abc\ldots kl$$

l'une des permutations des n lettres $a, b, c, \ldots k, l$; si l'on efface la lettre a qui occupe la première place, et qu'on l'écrive à droite de la dernière lettre l, on formera la nouvelle permutation

$$A_1 = bc\ldots kla,$$

et la substitution par laquelle on passe de la permutation A_0 à la permutation A_1 sera

$$\begin{pmatrix} A_1 \\ A_0 \end{pmatrix} = \begin{pmatrix} bc\ldots kla \\ abc\ldots kl \end{pmatrix}.$$

Pour effectuer cette substitution, il suffit évidemment de diviser la circonférence d'un cercle en n parties égales, d'écrire aux points de division successifs les lettres de la permutation A_0 et de remplacer chaque lettre par celle qui vient prendre sa place quand on fait tourner le cercle autour de son centre, dans un sens convenable, d'un angle égal à la $n^{\text{ième}}$ partie de quatre angles droits. C'est pour cette raison que la substitution dont nous nous occupons est dite *circulaire*.

Il est évident que *l'ordre d'une substitution circulaire est égal au nombre n des lettres qu'elle déplace*. En effet, chaque fois que le cercle dont il vient d'être question tourne d'une quantité angulaire égale à la $n^{\text{ième}}$ partie de quatre angles droits, la substitution s'effectue une fois. Or, pour ramener les choses à ce qu'elles étaient à l'origine, il faut que le cercle tourne, toujours dans le même sens, de n fois la $n^{\text{ième}}$ partie de quatre angles droits, et à ce moment la substitution a été effectuée n fois; donc l'ordre de la substitution est égal à n.

On représente habituellement une substitution circulaire en écrivant entre parenthèses l'une quelconque des permutations dont les lettres rangées en cercle sont tellement disposées que chacune d'elles remplace la précédente par l'effet de la substitution. Ainsi l'on a

$$\binom{bc\ldots kla}{abc\ldots kl} = (a, b, c, \ldots, k, l) = (b, c, \ldots, k, l, a) \ldots.$$

Décomposition d'une substitution quelconque en cycles.

408. Théorème I. — *Toute substitution, si elle n'est pas circulaire, est le produit de plusieurs substitutions circulaires effectuées sur des lettres différentes.*

En effet, soit S une substitution quelconque; exécu-

tons cette substitution. Soit a l'une des lettres qu'elle déplace et qu'elle remplace par une autre lettre b; b elle-même se trouvera remplacée par une troisième lettre c, et, en continuant de cette manière, on tombera nécessairement sur une lettre f qui se trouvera remplacée par a. Or il est évident que les lettres que l'on a ainsi rencontrées ont subi la substitution circulaire $(a, b, c, \ldots, f)$. En prenant une des lettres restantes, et opérant de la même manière, on formera un nouveau groupe de lettres qui auront subi une substitution circulaire, et l'on pourra continuer ainsi jusqu'à ce qu'on ait épuisé toutes les lettres que déplace la substitution S.

Si l'on désigne par C_0, C_1, C_2, ... les diverses substitutions circulaires que nous venons d'obtenir, on aura

$$S = C_0 C_1 C_2 \ldots,$$

formule qui exprime la valeur de S *décomposée en facteurs circulaires*. Ces facteurs sont dits les *cycles* de la substitution S. Les cycles qui ne contiennent que deux lettres prennent le nom de *transpositions* (n° 235).

Considérons, par exemple, la substitution

$$S = \begin{pmatrix} h\,k\,d\,f\,b\,j\,a\,g\,e\,c\,i \\ a\,b\,c\,d\,e\,f\,g\,h\,i\,j\,k \end{pmatrix};$$

en opérant comme nous l'avons indiqué, on trouvera

$$S = (a, h, g)(b, k, i, e)(c, d, f, j).$$

Lorsqu'une substitution S ne déplace pas quelques-unes des lettres du système que l'on considère, ces lettres ne figurent pas dans la valeur de S réduite à sa plus simple expression, ni dans les facteurs circulaires dont S est le produit. Si cependant on veut mettre ces lettres en évidence, on le pourra en introduisant dans S des cycles formés chacun avec une seule des lettres dont il s'agit,

et qui représentent évidemment des substitutions identiques; ainsi, dans le cas d'un système de six lettres a, b, c, d, e, f, la substitution

$$S = \begin{pmatrix} d\,c\,b\,a\,e\,f \\ a\,b\,c\,d\,e\,f \end{pmatrix}$$

pourra s'écrire

$$S = (a, d)\,(b, c)\,(e)\,(f).$$

409. Théorème II. — *L'ordre d'une substitution quelconque est égal au plus petit multiple commun des nombres qui expriment les ordres des cycles de la substitution.*

Soit

$$S = C_0\, C_1\, C_2 \ldots$$

la substitution S décomposée en cycles. Si ν désigne l'ordre de S, on aura

$$S^\nu = 1$$

ou

$$C_0^\nu\, C_1^\nu\, C_2^\nu \ldots = 1,$$

car il est évidemment permis d'intervertir l'ordre des facteurs circulaires de S^μ. Pour que la précédente égalité subsiste, il faut et il suffit que l'on ait

$$C_0^\nu = 1, \quad C_1^\nu = 1, \quad C_2^\nu = 1, \quad \ldots;$$

or, si α_0 désigne l'ordre du cycle C_0, les seules puissances de C_0 qui se réduiront à 1 ont pour exposants $\alpha_0, 2\alpha_0, 3\alpha_0, \ldots$: donc ν est un multiple de α_0. On voit de même que l'égalité $S^\nu = 1$ exige que ν soit divisible par les ordres $\alpha_1, \alpha_2, \ldots$ des cycles $C_1, C_2, C_3, \ldots$, et comme cette condition est d'ailleurs suffisante, l'ordre de S est précisément égal au plus petit multiple commun des nombres $\alpha_0, \alpha_1, \alpha_2, \ldots$.

410. Une substitution est dite *régulière,* lorsqu'elle est circulaire ou composée de facteurs circulaires d'un même ordre. Toute substitution qui n'est pas dans ce cas est dite *irrégulière.*

THÉORÈME III. — *La puissance* $\mu^{\text{ième}}$ *d'une substitution circulaire* S *d'ordre* ν *est elle-même circulaire si* μ *est premier à* ν. *Mais, si les nombres* μ *et* ν *ont un plus grand commun diviseur* θ *supérieur à* 1, S^μ *sera une substitution régulière composée de* θ *cycles d'ordre* $\frac{\nu}{\theta}$.

En effet, disposons, comme nous l'avons déjà fait plus haut, les ν lettres de la substitution circulaire S aux points de division d'une circonférence partagée en ν parties égales. La substitution S^μ aura pour effet de remplacer chaque lettre par celle qui en est éloignée d'une quantité égale à μ fois la $\nu^{\text{ième}}$ partie de la circonférence. Si donc, partant de l'un quelconque des points de division et marchant dans le même sens jusqu'à ce qu'on soit revenu au point de départ, on considère les points de division de μ en μ, les lettres placées à ces différents points devront subir par l'effet de S^μ une substitution circulaire. Or le nombre x de ces lettres doit être tel, que le produit de $\mu\frac{2\pi}{\nu}$ par x soit le plus petit multiple possible de 2π, ou, en d'autres termes, tel que μx soit le plus petit des nombres divisibles par ν; si donc θ désigne le plus grand commun diviseur des nombres μ et ν, on aura $x = \frac{\nu}{\theta}$. Il résulte évidemment de là que la substitution S^μ est le produit de θ substitutions circulaires renfermant chacune $\frac{\nu}{\theta}$ lettres. Si μ et ν sont premiers entre eux, on a $\theta = 1$ et la substitution S^μ est circulaire.

Exemple. — Considérons la substitution circulaire du sixième ordre

$$S = (a, b, c, d, e, f),$$

les puissances de cette substitution seront

$$\begin{aligned}
S &= (a, b, c, d, e, f),\\
S^2 &= (a, c, e)(b, d, f),\\
S^3 &= (a, d)(b, e)(c, f),\\
S^4 &= (a, e, c)(b, f, d),\\
S^5 &= (a, f, e, d, c, b),\\
S^6 &= 1.
\end{aligned}$$

411. Théorème IV. — *Réciproquement, toute substitution régulière est une puissance d'une substitution circulaire.*

En effet, soit la substitution régulière

$$S = (a_1, b_1, \ldots, g_1)(a_2, b_2, \ldots, g_2)\ldots(a_\theta, b_\theta, \ldots, g_\theta),$$

composée de θ cycles d'ordre $\frac{\nu}{\theta}$; il est évident que, si l'on fait

$$C = (a_1, a_2, \ldots, a_\theta, b_1, b_2, \ldots, b_\theta, \ldots, g_1, g_2, \ldots, g_\theta),$$

on aura

$$S = C^\theta.$$

Décomposition d'une substitution donnée en facteurs primitifs.

412. Les propriétés qu'il nous reste à établir dans ce Chapitre sont dues pour la plupart à Cauchy, qui les a fait connaître dans le tome III de ses *Exercices d'Analyse et de Physique mathématique*.

Soit S l'une quelconque des substitutions que l'on

peut former avec n lettres. Décomposons l'ordre ν de S en facteurs premiers, de manière que l'on ait

$$\nu = \alpha\beta\gamma \ldots,$$

α, β, γ, ... représentant des puissances de nombres premiers inégaux. Désignons par ν' le quotient de ν par α, c'est-à-dire le produit $\beta\gamma\ldots$, et par μ un entier quelconque positif ou négatif. Les nombres α et ν' étant premiers entre eux, on pourra trouver deux entiers positifs ou négatifs x et μ' tels, que l'on ait

$$\mu = \nu' x + \alpha\mu' \quad \text{ou} \quad \frac{\mu}{\nu} = \frac{x}{\alpha} + \frac{\mu'}{\nu'};$$

pareillement, si l'on désigne par ν'' le quotient de ν' par β, on pourra trouver deux entiers y et μ'' tels, que

$$\mu' = \nu'' y + \beta\mu'' \quad \text{ou} \quad \frac{\mu'}{\nu'} = \frac{y}{\beta} + \frac{\mu''}{\nu''};$$

on aura par suite

$$\frac{\mu}{\nu} = \frac{x}{\alpha} + \frac{y}{\beta} + \frac{\mu''}{\nu''},$$

et il est évident que, si le nombre ν'' est égal à 1, on pourra faire $\mu'' = 0$. En continuant ainsi, on mettra la fraction $\frac{\mu}{\nu}$ sous la forme

$$\frac{\mu}{\nu} = \frac{x}{\alpha} + \frac{y}{\beta} + \frac{z}{\gamma} + \ldots,$$

$x, y, z, \ldots$ étant des entiers. L'égalité précédente a lieu, quel que soit μ; et en faisant $\mu = 1$, on aura

$$1 = \frac{\nu}{\alpha} x + \frac{\nu}{\beta} y + \frac{\nu}{\gamma} z + \ldots.$$

D'après cela, la substitution donnée S pourra s'écrire

$$S = S^{\frac{\nu}{\alpha} x + \frac{\nu}{\beta} y + \frac{\nu}{\gamma} z + \ldots} = S^{\frac{\nu}{\alpha} x} S^{\frac{\nu}{\beta} y} S^{\frac{\nu}{\gamma} z} \ldots,$$

et si l'on fait, pour abréger,

$$S^{\frac{\nu}{\alpha}} = P, \quad S^{\frac{\nu}{\beta}} = Q, \quad S^{\frac{\nu}{\gamma}} = R, \quad \ldots,$$

on aura

$$S = P^x Q^y R^z \ldots.$$

La substitution S étant d'ordre ν, on voit que P est de l'ordre α, Q de l'ordre β, R de l'ordre γ, et ainsi de suite, D'ailleurs $x, y, z, \ldots$ sont premiers respectivement à $\alpha, \beta, \gamma, \ldots$; donc $P^x, Q^y, R^z, \ldots$ sont respectivement des ordres $\alpha, \beta, \gamma, \ldots$.

La formule précédente donne ainsi la valeur de S décomposée en facteurs qui ont respectivement pour ordres les puissances de nombres premiers dont l'ordre de S est le produit, et il est évident qu'on peut écrire ces facteurs dans un ordre quelconque, puisqu'ils sont tous des puissances de la substitution S.

Une substitution est dite *primitive,* lorsqu'elle a pour ordre un nombre premier ou une puissance d'un nombre premier. Si une substitution primitive est de l'ordre $\alpha = p^\lambda$, p étant un nombre premier, l'ordre de l'un quelconque de ses cycles qui est un diviseur de p^λ ne peut être que l'un des nombres $1, p, p^2, \ldots, p^{\lambda-1}$. On voit par ce qui précède que toute substitution est décomposable en un produit de substitutions primitives échangeables entre elles.

Exemple. — Considérons la substitution circulaire de six lettres

$$S = (a, b, c, d, e, f);$$

l'ordre de S est ici égal à 2×3. On a

$$S = S^3 . S^{-2} = S^3 . S^4;$$

en sorte que S^3 et S^4 sont les substitutions primitives

dont S est le produit. On a

$$S^3 = (a, d)(b, e)(c, f),$$
$$S^4 = (a, e, c)(b, f, d).$$

Des substitutions semblables.

413. Deux substitutions sont dites *semblables* entre elles quand elles offrent le même nombre de facteurs circulaires et le même nombre de lettres dans les cycles correspondants.

Il résulte de là que deux substitutions circulaires de même ordre sont semblables ; pareillement, deux substitutions régulières de même ordre sont semblables lorsqu'elles offrent le même nombre de facteurs circulaires.

Théorème. — *Si* S *et* S′ *désignent deux substitutions semblables, il existe une substitution* P *telle, que*

$$S'P = PS \quad \text{ou} \quad S' = PSP^{-1};$$

et réciproquement, s'il existe une substitution P *telle, que la précédente égalité ait lieu, les substitutions* S *et* S′ *sont semblables.*

Soit

$$S = \begin{pmatrix} B \\ A \end{pmatrix},$$

A et B désignant deux des permutations des n lettres a, b, c, ..., k, l. Supposons que a', b', c', ..., k', l' représentent ces mêmes lettres écrites dans un autre ordre quelconque, et soient A′ et B′ ce que deviennent A et B quand on y accentue les lettres. Il est clair que toute substitution S′ semblable à S pourra être représentée par

$$S' = \begin{pmatrix} B' \\ A' \end{pmatrix}.$$

Si, en outre, on désigne par P la substitution dont

l'effet est l'*accentuation* des lettres, on aura évidemment

$$P = \begin{pmatrix} A' \\ A \end{pmatrix} = \begin{pmatrix} B' \\ B \end{pmatrix} \quad \text{et} \quad P^{-1} = \begin{pmatrix} A \\ A' \end{pmatrix} = \begin{pmatrix} B \\ B' \end{pmatrix}.$$

Il résulte de là que

$$PSP^{-1} = \begin{pmatrix} B' \\ B \end{pmatrix} \begin{pmatrix} B \\ A \end{pmatrix} \begin{pmatrix} A \\ A' \end{pmatrix};$$

la substitution $\begin{pmatrix} A \\ A' \end{pmatrix}$ doit être effectuée la première; elle remplace les lettres de A' par celles de A, puis la deuxième substitution remplace A par B et la troisième B par B'; on a donc

$$PSP^{-1} = \begin{pmatrix} B' \\ A' \end{pmatrix} \quad \text{ou} \quad S' = PSP^{-1},$$

et, en multipliant à droite, de part et d'autre, par P,

$$S'P = PS.$$

Réciproquement, si la précédente égalité a lieu, la substitution S' est semblable à S. En effet, la substitution S étant toujours représentée par $\begin{pmatrix} B \\ A \end{pmatrix}$ et la substitution P par $\begin{pmatrix} A' \\ A \end{pmatrix}$ ou $\begin{pmatrix} B' \\ B \end{pmatrix}$, on a, par hypothèse,

$$S' = PSP^{-1}$$

ou

$$S' = \begin{pmatrix} B' \\ B \end{pmatrix} \begin{pmatrix} B \\ A \end{pmatrix} \begin{pmatrix} A \\ A' \end{pmatrix} = \begin{pmatrix} B' \\ A' \end{pmatrix};$$

d'où il suit que S' est semblable à S.

Corollaire I. — *La substitution* PSP^{-1}, *semblable à* S, *s'obtient en exécutant la substitution* P *dans les cycles de* S.

En effet, il est évident que cette opération équivaut à l'accentuation des lettres, dont nous avons fait usage dans la démonstration qui précède.

Corollaire II. — *Les produits* ST *et* TS, *que l'on obtient en multipliant entre elles deux substitutions quelconques* S *et* T, *sont des substitutions semblables.*

En effet, soient

$$ST = P, \quad TS = Q;$$

si l'on multiplie à droite par T^{-1} la première de ces égalités, il vient

$$S = PT^{-1},$$

et, en substituant dans la deuxième égalité, il vient

$$Q = TPT^{-1},$$

d'où il suit que les substitutions P et Q sont semblables.

Exemple. — Supposons que, le nombre des lettres étant six, on fasse

$$S = (a, b, c, d)(e, f), \quad T = (a, b, c)(d, e, f),$$

on aura les deux substitutions semblables du cinquième ordre

$$ST = (a, c, b, d, f)(e), \quad TS = (a, c, e, d, b)(f).$$

Du nombre des substitutions semblables à une substitution donnée.

414. Le nombre des lettres que l'on considère étant représenté par n, soit S une substitution contenant m_1 cycles de l'ordre n_1, m_2 cycles de l'ordre n_2, ..., enfin m_ω cycles de l'ordre n_ω; on aura

$$n = m_1 n_1 + m_2 n_2 + \ldots + m_\omega n_\omega,$$

chacun des nombres $n_1, n_2, \ldots, n_\omega$ pouvant se réduire à l'unité.

Nous commencerons par chercher le nombre des formes distinctes que l'on peut attribuer à la substitution S, décomposée en cycles, sans déplacer les parenthèses qui

renferment chaque cycle et sans altérer, en conséquence, le nombre des lettres contenues dans un facteur circulaire de rang déterminé. Il est clair que les seuls changements que l'on pourra faire ainsi sans altérer S consisteront à échanger entre eux les facteurs circulaires d'un même ordre, ou à faire passer successivement à la première place, dans chaque facteur circulaire, une quelconque des lettres contenues dans ce facteur. On voit, d'après cela, que le nombre M des formes diverses que l'on peut attribuer à S est

$$M = 1.2\ldots m_1 \cdot 1.2\ldots m_2 \ldots 1.2\ldots m_\omega \, n_1^{m_1} n_2^{m_2} n_\omega^{m_\omega}.$$

Soit maintenant $\mathfrak{N}$ le nombre des substitutions distinctes S, S′, S″, ... semblables à S. Si l'on écrit successivement chacune de ces substitutions sous les M formes distinctes qu'on peut lui attribuer sans déplacer les parenthèses, puis qu'on supprime ces parenthèses, on formera $M\mathfrak{N}$ permutations. Mais il est évident que, par ce procédé, aucune permutation des n lettres n'a été omise, et l'on a, en conséquence,

$$M\mathfrak{N} = 1.2.3\ldots n = N,$$

d'où

$$\mathfrak{N} = \frac{N}{M}.$$

Des substitutions échangeables entre elles.

415. Deux substitutions qui se réduisent à des puissances d'une même substitution sont échangeables entre elles; la même chose a lieu évidemment pour deux substitutions qui n'ont aucune lettre commune. Mais il importe de connaître la condition générale à laquelle doivent satisfaire deux substitutions échangeables; c'est ce dont nous allons nous occuper.

Soient S et T deux substitutions que nous supposons échangeables entre elles; on aura

$$ST = TS \quad \text{ou} \quad S = TST^{-1}.$$

Nous avons vu que la substitution TST^{-1} se déduit de la substitution S en exécutant dans les cycles de celle-ci la substitution T; donc, pour que les substitutions S et T soient échangeables entre elles, il faut et il suffit que la substitution S reste la même quand on exécute sur les lettres de ses cycles la substitution T. En conséquence, la substitution T ne peut produire sur S que des échanges entre des cycles d'un même ordre, et, dans un même cycle, le simple déplacement qui permet d'amener une lettre quelconque à la première place, sans altérer l'*ordre circulaire* des lettres du cycle. Chacun de ces échanges dont nous venons de parler, entre des cycles d'un même ordre, équivaut, s'il n'est pas *circulaire,* à plusieurs échanges circulaires effectués simultanément sur des cycles différents. Soient (C_0), (C_1), ..., $(C_{\mu-1})$ des cycles de même ordre qui doivent être ainsi échangés circulairement. La substitution T peut avoir, en outre, pour effet, comme nous venons de le dire, le déplacement qui permet d'amener une lettre quelconque à la première place dans chacun de ces cycles; mais l'arrangement C_0 par lequel se forme le cycle (C_0) ayant été choisi à volonté, on peut toujours prendre, pour former le cycle (C_1), l'arrangement C_1 que la substitution T doit mettre à la place de C_0; pareillement, pour former les cycles suivants (C_2), ..., $(C_{\mu-1})$, on peut choisir les arrangements C_2, ..., $C_{\mu-1}$ qui se substituent respectivement à C_1, C_2, ..., $C_{\mu-2}$. Quant au dernier arrangement $C_{\mu-1}$, il ne sera pas en général remplacé par C_0, mais par un autre arrangement C'_0 tel, que les cycles (C_0) et (C'_0) soient identiques.

Il résulte de là que, si l'on pose

$$P = C_0 \; C_1 \ldots C_{\mu-1}, \quad Q = \begin{pmatrix} C_1 \, C_2 \, \ldots C_{\mu-1} \, C'_0 \\ C_0 \, C_1 \, \ldots C_{\mu-2} \, C_{\mu-1} \end{pmatrix},$$

et que l'on désigne par P' et Q', P'' et Q'', ... des substitutions analogues à P et Q, mais relatives à des lettres différentes, on aura nécessairement

$$S = PP'P'' \ldots, \quad T = QQ'Q'' \ldots,$$

P et Q, P' et Q', P'' et Q'', ... étant des couples de substitutions échangeables entre elles, dont le nombre peut se réduire à l'unité.

416. Nous sommes ainsi ramenés à étudier les deux substitutions P et Q; la première est une substitution régulière, et on va voir que la deuxième l'est aussi.

Soit i l'ordre des cycles de P; pour plus de clarté, nous représenterons les lettres qui figurent dans un même cycle par un même *caractère* affecté des indices $0, 1, 2, \ldots, (i-1)$; posons donc

$$\begin{aligned} C_0 &= a_0 a_1 a_2 a_3 \ldots a_{i-1}, \\ C_1 &= b_0 b_1 b_2 b_3 \ldots b_{i-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots, \\ C_{\mu-2} &= e_0 e_1 e_2 e_3 \ldots e_{i-1}, \\ C_{\mu-1} &= f_0 f_1 f_2 f_3 \ldots f_{i-1}, \end{aligned}$$

et convenons, en outre, que l'un des caractères $a, b, \ldots, e, f$ affecté de l'indice $iq + \alpha$ désignera la même lettre que si l'indice était réduit au reste α de la division de $iq+\alpha$ par i. D'après cette convention, nous pouvons poser

$$C'_0 = a_\rho a_{\rho+1} a_{\rho+2} \ldots a_{\rho+i-1};$$

lorsque le nombre ρ est zéro, on a $C'_0 = C_0$ et alors, si l'on pose

$$(G_\xi) = (a_\xi, \; b_\xi, \; c_\xi, \; \ldots, \; e_\xi, \; f_\xi),$$

on aura évidemment

$$Q = (G_0)(G_1)(G_2)\ldots(G_{i-1}).$$

Mais supposons que ρ ne soit pas nul. Comme dans le cas que nous venons d'examiner, la substitution Q remplacera chacune des $\mu - 1$ premières lettres de l'arrangement

$$a_\xi b_\xi c_\xi \ldots e_\xi f_\xi$$

par celle qui la suit; quant à la dernière lettre f_ξ, elle sera remplacée par $a_{\xi+\rho}$, et chacune des $\mu - 1$ premières lettres de l'arrangement

$$a_{\xi+\rho} b_{\xi+\rho} \ldots e_{\xi+\rho} f_{\xi+\rho}$$

sera remplacée par la suivante, tandis que la lettre $f_{\xi+\rho}$ le sera par $a_{\xi+2\rho}$, et ainsi de suite. Le cercle se fermera nécessairement, mais cela ne pourra arriver que quand on aura rencontré la lettre $f_{\xi+(\lambda-1)\rho}$, dont l'indice est tel que $\lambda\rho$ soit divisible par i. On voit, d'après cela, que l'on obtiendra un cycle de Q en écrivant à la suite les uns des autres les λ arrangements

$$\begin{array}{l} a_\xi b_\xi \ldots\ldots f_\xi, \\ a_{\xi+\rho} b_{\xi+\rho} \ldots f_{\xi+\rho}, \\ \ldots\ldots\ldots\ldots, \\ a_{\xi+(\lambda-1)\rho} \ldots f_{\xi+(\lambda-1)\rho}. \end{array}$$

Désignons ce cycle par G_ξ; il reste à trouver le nombre des cycles G_ξ.

Or λ est, par définition, le plus petit nombre entier tel que $\lambda\rho$ soit divisible par i; $\lambda\rho$ est donc le plus petit commun multiple de ρ et de i, et par suite, si l'on appelle θ le plus grand commun diviseur de ρ et de i, on aura

$$\lambda = \frac{i}{\theta}:$$

chacun des cycles G_ξ contenant $\frac{i}{\theta}$ lettres a, leur nombre total est égal à θ, et l'on aura évidemment

$$Q = (G_0)(G_1)(G_2)\ldots(G_{\theta-1}).$$

De ce qui précède on peut conclure une règle très-simple pour obtenir les expressions des deux substitutions échangeables P et Q. Le nombre ρ étant pris arbitrairement et θ désignant toujours le plus grand commun diviseur de ρ et de i, formons le tableau

$$\begin{array}{llll}
a_\xi, & a_{\xi+1}, & \ldots, & a_{\xi+\theta-1}, \\
b_\xi, & b_{\xi+1}, & \ldots, & b_{\xi+\theta-1}, \\
\ldots & \ldots & \ldots & \ldots, \\
e_\xi, & e_{\xi+1}, & \ldots, & e_{\xi+\theta-1}, \\
f_\xi, & f_{\xi+1}, & \ldots, & f_{\xi+\theta-1},
\end{array}$$

composé de μ lignes horizontales et de θ colonnes verticales; désignons par

$$\mathcal{A}_\xi,\quad \mathcal{B}_\xi,\quad \ldots,\quad \mathcal{E}_\xi,\quad \mathcal{F}_\xi$$

les arrangements formés par les lignes horizontales et par

$$\mathcal{M}_\xi,\quad \mathcal{M}_{\xi+1},\quad \ldots,\quad \mathcal{M}_{\xi+\theta-1}$$

les arrangements formés par les lignes verticales, on aura les expressions suivantes des cycles de P et de Q :

$$\begin{array}{ll}
C_0 & = (\mathcal{A}_0\,\mathcal{A}_\theta\,\mathcal{A}_{2\theta}\ldots\mathcal{A}_{(\lambda-1)\theta}), \\
C_1 & = (\mathcal{B}_0\,\mathcal{B}_\theta\,\mathcal{B}_{2\theta}\ldots\mathcal{B}_{(\lambda-1)\theta}), \\
\ldots & \ldots\ldots\ldots\ldots\ldots\ldots, \\
C_{\mu-2} & = (\mathcal{E}_0\,\mathcal{E}_\theta\,\mathcal{E}_{2\theta}\ldots\mathcal{E}_{(\lambda-1)\theta}), \\
C_{\mu-1} & = (\mathcal{F}_0\,\mathcal{F}_\theta\,\mathcal{F}_{2\theta}\ldots\mathcal{F}_{(\lambda-1)\theta}),
\end{array}$$

et

$$\begin{aligned}
G_0 &= \mathcal{M}_0\,\mathcal{M}_\rho\,\mathcal{M}_{2\rho}\ldots\ldots\mathcal{M}_{(\lambda-1)\rho},\\
G_1 &= \mathcal{M}_1\,\mathcal{M}_{\rho+1}\,\mathcal{M}_{2\rho+1}\ldots\mathcal{M}_{(\lambda-1)\rho+1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
G_{\theta-2} &= \mathcal{M}_{\theta-2}\,\mathcal{M}_{\theta-2+\rho}\ldots\mathcal{M}_{\theta-2+(\lambda-1)\rho},\\
G_{\theta-1} &= \mathcal{M}_{\theta-1}\,\mathcal{M}_{\theta-1+\rho}\ldots\mathcal{M}_{\theta-1+(\lambda-1)\rho}.
\end{aligned}$$

Le nombre total j des lettres de chaque cycle G est

$$j = \lambda\mu.$$

Si $\rho = i$, on a $\lambda = 1$ et $j = \mu$; ce cas de $\rho = i$ équivaut à celui de $\rho = 0$ que nous avons examiné à part; il est, comme on le voit, compris dans le cas général.

Si ρ est un diviseur de i, on a $\theta = \rho$.

Si ρ et i sont premiers entre eux, on a $\theta = 1$, $\lambda = i$.

La substitution Q est formée des θ cycles (G) contenant chacun $\lambda\mu$ lettres; elle est par conséquent de l'ordre $\lambda\mu$ ou $\frac{\mu i}{\theta}$. On peut former sa puissance $\mu^{\text{ième}}$ qui sera de l'ordre λ. On déduit des expressions des cycles (G_ξ)

$$\begin{aligned}
&= (a_0, a_\rho, a_{2\rho}, \ldots, a_{(\lambda-1)\rho})(b_0, b_\rho, \ldots, b_{(\lambda-1)\rho})\ldots(f_0, f_\rho, \ldots, f_{(\lambda-1)\rho}),\\
&= (a_1, a_{\rho+1}, \ldots, a_{(\lambda-1)\rho+1})\\
&\quad\times(b_1, b_{\rho+1}, \ldots, b_{(\lambda-1)\rho+1})\ldots(f_1, f_{\rho+1}, \ldots, f_{(\lambda-1)\rho+1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
(G_{\theta-1})^\mu &= (a_{\theta-1}, a_{\rho+\theta-1}, \ldots, a_{(\lambda-1)\rho+\theta-1})\\
&\quad\times(b_{\theta-1}, b_{\rho+\theta-1}, \ldots, b_{(\lambda-1)\rho+\theta-1})\ldots(f_{\theta-1}, f_{\rho+\theta-1}, \ldots, f_{(\lambda-1)\rho+\theta-1}).
\end{aligned}$$

Les cycles contenant les lettres a qui figurent dans le produit

$$P^\mu = (G_0)^\mu (G_1)^\mu \ldots (G_{\theta-1})^\mu$$

constituent évidemment une substitution régulière qui est la puissance ρ du cycle (C_0). En étendant les mêmes

conclusions aux cycles formés des lettres b, c, ..., on obtient la formule

$$(G_0)^\mu (G_1)^\mu \ldots (G_{\theta-1})^\mu = (C_0)^\rho (C_1)^\rho \ldots (C_{\mu-1})^\rho$$

ou

$$P^\rho = Q^\mu.$$

417. Comme application prenons

$$C_0 = a_0\, a_1\, a_2\, a_3\, a_4\, a_5,$$
$$C_1 = b_0\, b_1\, b_2\, b_3\, b_4\, b_5,$$
$$C_2 = c_0\, c_1\, c_2\, c_3\, c_4\, c_5,$$
$$C_3 = d_0\, d_1\, d_2\, d_3\, d_4\, d_5.$$

On a ici

$$i = 6, \quad \mu = 4.$$

Prenons $\rho = 4$, et par suite

$$\theta = 2, \quad \lambda = 3,$$

on aura

$$\mathcal{A}_\xi = a_\xi\, a_{\xi+1}, \quad \mathcal{M}_\xi = a_\xi\, b_\xi\, c_\xi\, d_\xi,$$
$$G_0 = (a_0, b_0, c_0, d_0, a_4, b_4, c_4, d_4, a_2, b_2, c_2, d_2),$$
$$G_1 = (a_1, b_1, c_1, d_1, a_5, b_5, c_5, d_5, a_3, b_3, c_3, d_3).$$

Les deux substitutions P et Q ont pour expressions

$$P = C_0\, C_1\, C_2\, C_3,$$
$$Q = G_0\, G_1,$$

et il est aisé de vérifier que l'on a

$$P^4 = Q^4 = (a_0, a_4, a_2)(a_1, a_5, a_3)(b_0, b_4, b_2)(b_1, b_5, b_3)$$
$$\times (c_0, c_4, c_2)(c_1, c_5, c_3)(d_0, d_4, d_2)(d_1, d_5, d_3).$$

On a d'ailleurs

$$PQ = QP = (a_0, b_1, c_2, d_3, a_2, b_3, c_4, d_5, a_4, b_5, c_0, d_1)$$
$$\times (a_1, b_2, c_3, d_4, a_3, b_4, c_5, d_0, a_5, b_0, c_1, d_2).$$

Remarquons d'ailleurs que la substitution P étant

du sixième ordre, de l'égalité évidente

$$P^8 = Q^8,$$

on déduit

$$P^2 = Q^6.$$

Une remarque semblable s'applique au cas général. On a

$$P^\rho = Q^\mu,$$

et par conséquent, x étant un entier quelconque,

$$P^{x\rho} = Q^{x\mu}.$$

Déterminons cet entier x par la congruence

$$x\rho \equiv \theta \pmod{i},$$

toujours possible puisque θ est le plus grand commun diviseur de ρ et de i. On aura, la substitution P étant d'ordre i,

$$P^{x\rho} = P^\theta,$$

et par suite

$$P^\theta = Q^{x\mu}.$$

De cette équation on déduit encore, en se rappelant que Q est de l'ordre $\frac{i\mu}{\theta}$,

$$P^\theta = Q^{\left(x + n\frac{i}{\theta}\right)\mu},$$

n étant entier.

D'ailleurs, l'entier x étant défini par la congruence,

$$x\rho \equiv \theta \pmod{i}$$

ou

$$x\frac{\rho}{\theta} \equiv 1 \pmod{\frac{i}{\theta}}$$

sera premier avec $\frac{i}{\theta}$.

Les deux nombres x, $\frac{i}{\theta}$ étant premiers entre eux, on pourra toujours déterminer un entier n de telle manière que $x + n\frac{i}{\theta}$ soit premier avec θ. Nous pourrons donc toujours supposer que dans l'équation

$$P^{\theta} = Q^{x\mu}$$

θ et x sont premiers entre eux.

418. L'analyse précédente, qui nous donne la composition de deux substitutions échangeables S et T, doit nous présenter les deux cas dont nous avons fait mention au n° 415, savoir le cas où les substitutions S et T ne déplacent pas les mêmes lettres, et celui où S et T sont des puissances d'une même substitution. Le premier de ces deux cas se présente quand l'une des deux substitutions P et Q, P' et Q', P'' et Q'', ... se réduit à l'unité. Or, pour qu'il en soit ainsi à l'égard de P et Q, il faut et il suffit évidemment que l'un des nombres i et j soit égal à l'unité. Quant au deuxième cas, il est facile d'établir cette proposition :

Pour que les substitutions P *et* Q *soient des puissances d'une même substitution, il faut et il suffit que les nombres* μ *et* θ *n'aient aucun diviseur commun autre que l'unité.*

Supposons que l'on ait

$$(1) \qquad P = R^{\alpha}, \quad Q = R^{\beta},$$

la substitution R sera circulaire, car les lettres a_{ξ}, $a_{\xi+1}$, ..., $a_{\xi+\lambda\rho-1}$ doivent figurer dans un même cycle de R, puisqu'elles constituent un cycle de R^{α} ou P; pareillement les lettres a_{ξ}, b_{ξ}, ..., f_{ξ} figurent dans un même cycle de R^{β} ou Q; donc elles appartiennent,

dans la substitution R, au même cycle que les lettres précédentes. Ce cycle renferme donc toutes les μi lettres; en conséquence, la substitution R est circulaire et d'ordre μi. D'ailleurs R^α est de l'ordre i, R^6 de l'ordre $\frac{\mu i}{\theta}$; par suite α et β sont respectivement divisibles par μ et par θ (n° 406). Si donc μ et θ ont un diviseur commun δ supérieur à 1, α et β admettront ce diviseur, et si l'on pose

$$\alpha = \delta\alpha', \quad 6 = \delta 6',$$

puis

$$R' = R^\delta,$$

on aura

$$P = R'^{\alpha'}, \quad Q = R'^{6'},$$

ce qui est impossible, puisque la substitution R' n'est pas circulaire. Les équations (1) exigent donc que μ et θ soient premiers entre eux.

Supposons cette condition remplie. Nous avons vu que, dans l'égalité

$$P^\theta = Q^{x\mu},$$

on peut supposer x premier à θ; θ sera donc premier à $x\mu$ et l'on pourra trouver deux nombres entiers u, t, tels que

$$u\theta + tx\mu = 1;$$

et si l'on pose

$$R = P^t Q^u,$$

on aura

$$P = R^{x\mu}, \quad Q = R^\theta.$$

Exemple. — Considérons les deux substitutions

$$P = (a_0, a_1, a_2, a_3, a_4, a_5)(b_0, b_1, b_2, b_3, b_4, b_5)(c_0, c_1, c_2, c_3, c_4, c_5),$$
$$Q = (a_0, b_0, c_0, a_4, b_4, c_4, a_2, b_2, c_2)(a_1, b_1, c_1, a_5, b_5, c_5, a_3, b_3, c_3).$$

On a ici $\mu = 3$, $i = 6$, $\rho = 4$, $\theta = 2$.

Le nombre x défini par la congruence

$$x\rho \equiv 5 \pmod{i}$$

a pour valeur $x = -1$; on a donc

$$P^4 = Q^3; \quad P^2 = Q^{3},$$

et en posant

$$R = P^{-1}Q = (a_0, b_5, c_4, a_1, b_0, c_5, a_2, b_1, c_0, a_3, b_2, c_1, a_4, b_3, c_2, a_5, b_4, c_3),$$

on trouve

$$Q = R^4, \quad P = R^3.$$

419. Supposons maintenant que l'on demande le nombre des substitutions échangeables avec une substitution donnée S. Soit T une telle substitution, on aura

$$S = TST^{-1},$$

et nous avons vu que la substitution TST^{-1} s'obtient, quel que soit T, en exécutant la substitution T dans les cycles de S; donc il y a autant de substitutions T satisfaisant à l'équation précédente qu'il y a de manières différentes d'exprimer S sans déplacer les parenthèses qui entourent les cycles, c'est-à-dire sans altérer le nombre des lettres contenues dans chaque cycle. Ce nombre est précisément celui qui a été représenté par M au n° **414**, et qui a pour valeur

$$M = (1.2\ldots m_1)(1.2\ldots m_2)\ldots(1.2\ldots m_\omega)\, n_1^{m_1} n_2^{m_2} \ldots n_\omega^{m_\omega};$$

m_i désigne le nombre des cycles d'ordre n_i dans la substitution S, et n étant le nombre total des lettres, on a

$$n = m_1 n_1 + m_2 n_2 + \ldots + m_\omega n_\omega.$$

420. Nous terminerons l'étude des substitutions échangeables entre elles, en démontrant deux propositions importantes qui nous seront utiles dans la suite.

Théorème I. — *Si* T, U, V, ..., W *sont des substi-*

tutions échangeables avec une substitution donnée S, *le produit* TU, ..., *obtenu en multipliant entre elles plusieurs des substitutions* T, U, ..., *sera également une substitution échangeable avec* S.

En effet, on a, par hypothèse,

$$T = STS^{-1}, \quad U = SUS^{-1},$$

et, en multipliant,

$$TU = STS^{-1}\,SUS^{-1};$$

les deux facteurs consécutifs S et S^{-1} peuvent être remplacés par leur produit 1 dans le second membre; on a donc

$$TU = STUS^{-1} \quad \text{ou} \quad TU = S \times TU \times S^{-1},$$

ce qui montre que la substitution TU est échangeable avec S. On en conclut immédiatement que toutes les substitutions de la forme TUV... sont pareillement échangeables avec S.

421. Théorème II. — *Si m désigne un nombre premier avec l'ordre d'une substitution donnée* S, *il existe des substitutions qui satisfont à l'égalité*

$$(1) \qquad S^m = TST^{-1},$$

et leur nombre est précisément égal au nombre des substitutions qui sont échangeables avec S.

Remarquons d'abord que l'égalité $S^m = TST^{-1}$ ne peut avoir lieu que si m est premier avec l'ordre de S, car les substitutions TST^{-1} et S sont semblables et, en conséquence, du même ordre; d'ailleurs S et S^m ne peuvent être du même ordre que si m est premier avec l'ordre de S.

Cela posé, soient (C) l'un quelconque des cycles de S et $(\Gamma) = (C)^m$ la puissance $m^{\text{ième}}$ de ce cycle; il est

évident que l'égalité (1) sera satisfaite si l'on prend

$$T = \Theta = \binom{\Gamma}{C};$$

$\binom{\Gamma}{C}$ désignant, pour abréger, la substitution qui remplace tous les arrangements C par les correspondants Γ; en effet, la substitution $\Theta S \Theta^{-1}$ s'obtient en remplaçant les arrangements C contenus dans les cycles de S par les correspondants Γ; on a donc

$$S^m = \Theta S \Theta^{-1}.$$

D'après cela l'égalité (1) peut s'écrire

$$(2) \qquad TST^{-1} = \Theta S \Theta^{-1},$$

et si l'on multiplie à gauche par Θ^{-1} et à droite par Θ, elle prend la forme

$$(3) \qquad \Theta^{-1} TST^{-1} \Theta = S;$$

enfin, si l'on pose

$$T = \Theta U, \quad \text{d'où} \quad T^{-1} = U^{-1}\Theta^{-1},$$

l'égalité (3) se réduit à

$$USU^{-1} = S,$$

d'où il suit que U est une substitution échangeable avec S.

Il résulte de là qu'on obtiendra toutes les solutions de l'équation (1), en multipliant par l'une d'elles Θ toutes les substitutions échangeables avec S; le nombre de celles-ci est donc égal au nombre des substitutions T.

Exemple. — Pour donner un exemple de ce théorème, reprenons les deux substitutions

$$P = (a_0, a_1, a_2, a_3)(b_0, b_1, b_2, b_3)(c_0, c_1, c_2, c_3),$$
$$Q = (a_0, b_0, c_0, a_2, b_2, c_2)(a_1, b_1, c_1, c_1, a_3, b_3, c_3)$$

que nous avons déjà considérées et qui sont des puissances d'une même substitution. Si l'on veut déduire de Q une substitution Q′ telle, que

$$P^3 = Q'PQ'^{-1},$$

il suffira de multiplier Q par la substitution dont les deux termes sont respectivement les arrangements qui constituent P^3 et P; on voit de suite que cette substitution est

$$\Theta = (a_1, a_3)\ (b_1, b_3)\ (c_1, c_3),$$

et l'on a

$$Q' = \Theta Q = (a_0, b_0, c_0, a_2, b_2, c_2)\,(a_1, b_3, c_1)\,(a_3, b_1, c_3).$$

Réduction d'une substitution quelconque à un produit de transpositions.

422. Toute substitution est équivalente à plusieurs transpositions. En effet, comme nous l'avons déjà dit au n° **235**, si, par l'effet de la substitution S, la lettre a doit prendre la place qui est occupée actuellement par b, il est évident que la substitution S équivaut à la transposition (a, b), jointe à une substitution S′ qui ne déplace que les lettres b...; en d'autres termes, on a

$$S = S' \times (a, b);$$

on peut raisonner sur S′ comme on vient de le faire sur S, et, en continuant de la même manière, on décomposera S en un produit de transpositions.

On peut réaliser une substitution S de plusieurs manières différentes, par le moyen de transpositions successives; mais, quelle que soit la marche que l'on aura suivie, le nombre des transpositions employées

sera toujours le même à un multiple de 2 près. Cela va résulter du théorème suivant :

Théorème. — *Si σ désigne le nombre des cycles d'une substitution* S, *relative à n lettres, le produit* TS *ou* ST, *obtenu en multipliant entre elles la substitution* S *et la transposition* T, *sera une substitution dans laquelle le nombre des cycles sera $\sigma \pm 1$, savoir : $\sigma + 1$ si les lettres de* T *appartiennent à des cycles différents de* S, *et $\sigma - 1$ dans le cas contraire.*

Soit

$$T = (a_1, b_1),$$

et supposons que les lettres a_1, b_1 appartiennent à deux cycles différents de S, savoir :

$$C = (a_1, a_2, \ldots, a_i), \quad C' = (b_1, b_2, \ldots, b_j).$$

Si l'on exécute la substitution S sur l'arrangement

$$a_1 a_2, \ldots a_{i-1}\, a_i\, b_1\, b_2 \ldots\; b_{j-1}\, b_j,$$

on obtiendra le nouvel arrangement

$$a_2\, a_3 \ldots\; a_i\, a_1\; b_2\, b_3 \ldots\; b_j\, b_1,$$

et, si l'on applique à celui-ci la transposition T, on obtient

$$a_2\, a_3 \ldots\; a_i\; b_1\; b_2\, b_3 \ldots\; b_j\, a_1\,;$$

en comparant cet arrangement à celui d'où l'on est parti, on trouve

$$TCC' = (a_1, a_2, \ldots a_i, b_1, b_2, \ldots, b_j);$$

la substitution TS renferme donc un cycle de moins que la substitution S, et la même chose peut se dire de ST qui est semblable à TS.

Supposons maintenant que les lettres a_1, b_1 fassent partie d'un même cycle C de S, et soit

$$C = (a_1, a_2, \ldots, a_i, b_1, b_2, \ldots, b_j).$$

Si l'on applique la substitution S à l'arrangement

$$a_1 a_2 \ldots a_{i-1} a_i b_1 b_2 \ldots b_{j-1} b_j,$$

on obtient

$$a_2 a_3 \ldots a_i b_1 b_2 b_3 \ldots b_j a_1,$$

et, en faisant la transposition T, il vient

$$a_2 a_3 \ldots a_i a_1 b_2 b_3 \ldots b_j b_1,$$

d'où il suit que l'on a

$$TC = (a_1, a_2, \ldots, a_i)(b_1, b_2, \ldots, b_j);$$

donc la substitution TS renferme un cycle de plus que la substitution S, et la même chose a lieu, en conséquence, à l'égard de la substitution ST.

Remarque. — Il est évident qu'il faut tenir compte, pour l'exactitude du théorème, des cycles qui se réduisent à une seule lettre.

Corollaire. — *Si σ désigne le nombre des cycles d'une substitution* S *formée avec n lettres, et que cette substitution puisse être obtenue en multipliant entre elles et dans un certain ordre ν transpositions égales ou inégales, on aura*

$$\nu = (n - \sigma) + 2k,$$

k étant un nombre entier.

En effet, la première transposition peut être regardée comme une substitution formée de $n - 1$ cycles, l'un du deuxième ordre et les $n - 2$ autres du premier ordre; donc, en la multipliant par la deuxième transposition, on

obtiendra une substitution qui sera formée de $n-1\pm 1$ cycles; ce premier produit, multiplié par la troisième transposition, donnera un nouveau produit dans lequel le nombre des cycles sera $n-1\pm 1\pm 1$, et ainsi de suite; en sorte que, après avoir exécuté la multiplication des ν transpositions, on se verra conduit à l'égalité

$$\sigma = n-1\pm 1\pm 1\pm\ldots\pm 1,$$

dans laquelle le nombre des unités positives ou négatives ajoutées à n sera égal à ν. Or, si l'on donne le signe — à l'une des unités qui doit avoir le signe $+$, on diminue de 2 unités le second membre de notre égalité. Il s'ensuit donc que l'on a

$$\sigma = n-\nu+2k \quad \text{ou} \quad \nu = (n-\sigma)+2k,$$

et, en conséquence, le nombre des transpositions successives par lesquelles on peut effectuer une substitution donnée S est toujours de même parité, quelle que soit la marche que l'on suive pour former les transpositions.

423. On peut, d'après cela, distinguer en deux genres les $N = 1.2\ldots n$ substitutions formées avec n lettres. Le premier genre comprendra les substitutions qui équivalent à un nombre pair de transpositions, tandis que celles qui équivalent à un nombre impair de transpositions constitueront le second genre.

Soient

$$1,\ S_1,\ S_2,\ S_3$$

les substitutions du premier genre, parmi lesquelles figure l'unité, et

$$T_0,\ T_1,\ T_2,\ T_3,\ \ldots$$

celles du deuxième genre. Il est évident que ces deux suites se changeront l'une dans l'autre, si on les multiplie

par une transposition (a, b); par conséquent, il y a $\frac{N}{2}$ substitutions de l'un et de l'autre genre.

On peut aussi énoncer les résultats suivants :

Une substitution circulaire est du premier ou du deuxième genre, suivant que son ordre ou le nombre de ses lettres est impair ou pair.

Le produit de plusieurs substitutions est du premier ou du deuxième genre, suivant que le nombre des facteurs du deuxième genre est pair ou impair.

Les puissances paires d'une substitution quelconque appartiennent au premier genre.

CHAPITRE II.

PROPRIÉTÉS DES SYSTÈMES DE SUBSTITUTIONS CONJUGUÉES.

Des systèmes conjugués.

424. Étant données plusieurs substitutions formées avec n lettres, si, en les multipliant une ou plusieurs fois les unes par les autres ou par elles-mêmes, dans un ordre quelconque, on n'obtient jamais que des substitutions comprises dans la suite des substitutions données, celles-ci constituent ce que Cauchy a nommé un *système de substitutions conjuguées*, ou simplement un *système conjugué*. Il est évident que tout système conjugué comprend la substitution égale à l'unité.

L'*ordre* d'un système conjugué est le nombre des substitutions qu'il renferme.

Il résulte de ces définitions que les $N = 1.2 \ldots n$ substitutions que l'on peut former avec n lettres constituent un système conjugué d'ordre N, et que les puissances d'une substitution quelconque d'ordre ν constituent un système de substitutions conjuguées d'ordre ν.

425. Théorème. — *Si toutes les substitutions d'un système conjugué* Γ *d'ordre* μ *sont comprises parmi les substitutions d'un autre système conjugué* G *d'ordre* m, *le nombre* μ *sera un diviseur de* m.

En effet, désignons par

$$(1) \qquad 1,\ S_1,\ S_2,\ S_3,\ \ldots,\ S_{\mu-1}$$

les μ substitutions du système Γ; ces substitutions appartiennent à G, par hypothèse, et l'on a $m > \mu$. Soit T_1 l'une des substitutions de G qui n'appartiennent pas au système Γ, c'est-à-dire à la suite (1); si l'on multiplie, à droite, par T_1 les termes de cette suite, les produits

(2) $$T_1,\ S_1T_1,\ S_2T_1, \ldots,\ S_{\mu-1}T_1,$$

que l'on obtiendra, seront compris parmi les substitutions du système G; d'ailleurs, deux quelconques de ces substitutions (2) sont évidemment distinctes et aucune d'elles ne saurait appartenir à la suite (1). Pour établir ce dernier point, il suffit de remarquer que l'égalité $S_iT_1 = S_j$ entraînerait $T_1 = S_i^{-1}S_j$, ce qui est impossible, car le produit $S_i^{-1}S_j$ appartient nécessairement au système Γ, tandis que, par hypothèse, T_1 ne fait pas partie de ce système : il résulte de là que l'on a $m = 2\mu$, ou $m > 2\mu$. Si m est égal à 2μ, le théorème est démontré; soit donc $m > 2\mu$, et désignons par T_2 l'une des substitutions de G qui n'appartiennent à aucune des suites (1) et (2). En multipliant à droite par T_2 les substitutions (1), on obtiendra μ substitutions nouvelles,

(3) $$T_2,\ S_1T_2,\ S_2T_2, \ldots,\ S_{\mu-1}T_2,$$

qui appartiendront au système G; elles seront distinctes entre elles et distinctes des substitutions (1); en outre, elles sont distinctes des substitutions (2), car l'égalité $S_iT_2 = S_jT_1$ entraînerait $T_2 = S_i^{-1}S_jT_1$, ce qui est contre l'hypothèse, car le produit $S_i^{-1}S_jT_1$ fait évidemment partie des substitutions (2). Il résulte de là que $m = 3\mu$ ou $m > 3\mu$. Il est clair que l'on peut poursuivre de cette manière jusqu'à ce que l'on ait épuisé toutes les substitutions du système G, et que l'on aura en conséquence

$$m = q\mu,$$

q désignant un nombre entier.

REMARQUE. — Le système conjugué G a été ainsi partagé en q *suites* de substitutions,

$$\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ T_1, & S_1T_1, & S_2T_1, & \ldots, & S_{\mu-1}T_1, \\ T_2, & S_1T_2, & S_2T_2, & \ldots, & S_{\mu-1}T_2, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T_{q-1}, & S_1T_{q-1}, & S_2T_{q-1}, & \ldots, & S_{\mu-1}T_{q-1}, \end{array}$$

dont la première seule constitue un système conjugué. Pour former ce tableau, sur lequel repose notre raisonnement, nous avons successivement multiplié, à droite, par les substitutions $T_1, T_2, \ldots, T_{q-1}$ les substitutions du système Γ; mais il faut remarquer que l'on aurait pu procéder d'une autre manière, et que la démonstration aurait pu être faite en employant des substitutions $U_1, U_2, \ldots, U_{q-1}$ du système G, comme multiplicateurs, à gauche, des substitutions du système Γ. En procédant ainsi, on aurait décomposé le système G en q suites formées chacune, comme les précédentes, de μ substitutions et qui sont

$$\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ U_1, & U_1S_1, & U_1S_2, & \ldots, & U_1S_{\mu-1}, \\ U_2, & U_2S_1, & U_2S_2, & \ldots, & U_2S_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ U_{q-1}, & U_{q-1}S_1, & U_{q-1}S_2, & \ldots, & U_{q-1}S_{\mu-1}, \end{array}$$

chaque substitution U étant choisie parmi les substitutions de G qui ne font pas partie des lignes horizontales déjà formées.

426. Le théorème que nous venons d'établir conduit à des conséquences importantes, qui sont contenues dans les corollaires suivants :

COROLLAIRE I. — *L'ordre d'un système de substitutions*

conjuguées formées avec n lettres est un diviseur du produit $N = 1.2.3 \ldots n$.

En effet, les substitutions du système proposé appartiennent au système conjugué de l'ordre N qui comprend toutes les substitutions.

Corollaire II. — *L'ordre d'un système de substitutions conjuguées est un multiple de l'ordre de l'une quelconque des substitutions du système.*

En effet, les puissances de l'une des substitutions d'un système conjugué appartiennent toutes à ce système; d'ailleurs, ces puissances constituent un système conjugué dont l'ordre est égal à celui de la substitution; donc cet ordre est un diviseur de l'ordre du système proposé.

Corollaire III. — *Le nombre n des lettres étant supposé premier, tout système conjugué d'ordre n se compose des n puissances d'une substitution circulaire d'ordre n.*

En effet, l'ordre d'une substitution quelconque du système doit diviser n; il se réduit donc à 1 ou à n.

Corollaire IV. — *Si deux systèmes conjugués offrent des substitutions communes, celles-ci constituent un système conjugué et leur nombre est en conséquence un diviseur commun des ordres des deux systèmes donnés.*

En effet, soient

$$(1) \qquad 1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1}$$

toutes les substitutions communes à deux systèmes conjugués. Toute substitution S, obtenue en multipliant les précédentes entre elles ou par elles-mêmes, appartient à la fois aux deux systèmes proposés; et, comme ceux-ci n'ont que les μ substitutions communes (1), il

est évident que la substitution S se trouve comprise parmi elles; ces substitutions communes constituent donc un système conjugué.

Des systèmes semblables et des systèmes échangeables entre eux.

427. Considérons un système de substitutions conjuguées

(1) $$1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1};$$

on a vu que TST^{-1} et S sont deux substitutions semblables, quelle que soit la substitution T, et que, pour former la substitution TST^{-1}, il suffit d'effectuer la substitution T dans les cycles de S; il en résulte que les substitutions

(2) $$1,\ TS_1T^{-1},\ TS_2T^{-1},\ \ldots,\ TS_{\mu-1}T^{-1}$$

constituent un système conjugué. On peut aussi vérifier immédiatement ce fait, en remarquant que le produit d'un nombre quelconque de substitutions prises dans la suite (2) est de la forme $TS_\alpha S_\beta \ldots S_\omega T^{-1}$, et par suite de la forme TS_iT^{-1}, puisque les substitutions (1) forment, par hypothèse, un système conjugué.

Les systèmes conjugués (1) et (2) seront dits *semblables* (¹); il peut arriver que ces deux systèmes coïncident, et alors on a, quel que soit i,

$$TS_iT^{-1} = S_j \quad \text{ou} \quad TS_i = S_jT;$$

par conséquent, on obtient les mêmes résultats en mul-

(¹) M. Betti a donné aux substitutions (2) le nom de *dérivées* des substitutions correspondantes (1); T est la *dérivante*, et le système (1) est alors le *dérivé par* T du système (1).

tipliant les substitutions (1) par T, soit à droite, soit à gauche.

Considérons maintenant deux systèmes de substitutions conjuguées,

$$1,\ S_1,\ S_2,\ S_3,\ \ldots,\ S_\mu$$
$$1,\ T_1,\ T_2,\ T_3,\ \ldots,\ T_{\nu-1};$$

nous dirons que ces deux systèmes sont *échangeables* entre eux lorsque tout produit de la forme $T_j S_i$ sera en même temps de la forme $S_{i'} T_{j'}$. Si l'on a $j'=j$, quels que soient i et j, le premier des deux systèmes proposés coïncidera avec le système semblable que l'on en déduit en multipliant ses substitutions à gauche par T_j et à droite par T_j^{-1}. Si l'on a en même temps $i'=i, j'=j$, quels que soient i et j, deux substitutions quelconques, prises dans les deux systèmes proposés, seront échangeables entre elles.

Du problème général qui fait l'objet principal de la théorie des substitutions.

428. Le problème général que l'on a en vue dans la théorie des substitutions peut être énoncé dans les termes suivants :

Quels sont les systèmes de substitutions conjuguées que l'on peut former avec n lettres données?

La solution de ce problème serait, pour l'Algèbre, de la plus haute importance; aussi Lagrange et, après lui, plusieurs géomètres éminents se sont-ils occupés de cette question difficile. Mais, malgré leurs efforts, ils n'ont pu atteindre le but proposé, et la Science ne possède aujourd'hui sur ce sujet qu'un petit nombre de propositions générales que nous allons établir ici.

Parmi les systèmes de substitutions conjuguées que l'on peut former avec n lettres données, nous connaissons : 1° le système qui comprend les $N = 1.2\ldots n$ substitutions; 2° les systèmes que l'on forme en prenant toutes les puissances d'une substitution quelconque. Nous les rappelons ici, afin de présenter un ensemble complet des résultats acquis.

429. Théorème I. — *Parmi les* $N = 1.2\ldots n$ *substitutions que l'on peut former avec n lettres données, celles qui équivalent à un nombre pair de transpositions constituent un système conjugué d'ordre* $\frac{N}{2}$, *et il n'existe aucun autre système conjugué du même ordre* $\frac{N}{2}$.

La première partie du théorème est évidente. Nous avons vu, en effet, que si l'on multiplie entre elles plusieurs substitutions du premier genre, c'est-à-dire plusieurs substitutions dont chacune équivaut à un nombre pair de transpositions, on obtient pour résultat une substitution du premier genre.

Pour établir la seconde partie, soit

$$(1) \qquad 1,\ S_1,\ S_2,\ S_3,\ \ldots,\ S_{\frac{N}{2}-1}$$

un système conjugué d'ordre $\frac{N}{2}$. Multiplions à gauche et à droite les substitutions de ce système par une substitution quelconque T, nous obtiendrons les produits

$$(2) \qquad T,\ TS_1,\ TS_2,\ \ldots,\ TS_{\frac{N}{2}-1},$$

et

$$(3) \qquad T,\ S_1T,\ S_2T,\ \ldots,\ S_{\frac{N}{2}-1}T.$$

Si T fait partie du système (1), les suites (2) et (3) formeront des systèmes conjugués identiques à (1); mais, si T n'est pas compris dans le système (1), chacune des suites (2) et (3) se composera, comme on l'a vu précédemment, des $\frac{N}{2}$ substitutions qui n'appartiennent pas au système (1). Dans tous les cas, les suites (2) et (3) offrent les mêmes substitutions, et l'on a, en conséquence, quel que soit i, pour une certaine valeur de j,

$$TS_i = S_j T \quad \text{ou} \quad TS_i T^{-1} = S_j;$$

d'où il résulte que le système (1) renferme toutes les substitutions semblables à l'une quelconque de celles qui y sont contenues. Ce système ne renferme donc aucune des transpositions; car autrement il les renfermerait toutes, et son ordre serait égal à N, ce qui est contre l'hypothèse.

Supposons que T désigne maintenant une transposition, les suites (1) et (2) comprendront toutes les N substitutions des n lettres, et ces substitutions ne feront que s'échanger entre elles, si on les multiplie par une transposition U. Or il est évident, d'après ce qui précède, que, par cette multiplication, la suite (1) se transformera dans la suite (2); donc à son tour la suite (2) se changera dans la suite (1), ce qui montre que la substitution UT fait partie du système (1). Ce système comprend ainsi toutes les substitutions que l'on obtient en multipliant deux transpositions entre elles, et il renferme, en conséquence, les $\frac{N}{2}$ substitutions qui équivalent chacune à un nombre pair quelconque de transpositions.

Corollaire. — *Le système conjugué d'ordre* $\frac{N}{2}$ *renferme toutes les substitutions circulaires d'ordre impair, et il n'en renferme aucune d'ordre pair.*

En effet, toute substitution circulaire d'ordre p équivaut à $p-1$ transpositions; on a

$$(a_0, a_1, a_2, \ldots, a_{p-1}) = (a_0, a_{p-1})(a_0, a_{p-2})\ldots(a_0, a_2)(a_0, a_1).$$

430. Théorème II. — *Si un système conjugué renferme toutes les substitutions circulaires dont l'ordre est un nombre donné p égal ou inférieur à n, l'ordre du système conjugué est N ou $\frac{N}{2}$. Cet ordre est toujours égal à N si p est pair.*

Le théorème est évident, dans le cas de $p=2$; car le système proposé contient toutes les transpositions et son ordre est égal à N. Dans le cas de $p=3$, le système proposé renferme la substitution circulaire

$$(a_1, a_2, a_3) = (a_1, a_3)(a_1, a_2)$$

des trois lettres données a_1, a_2, a_3 et il contient aussi la substitution

$$(a_4, a_3, a_1) = (a_3, a_4)(a_1, a_3),$$

si, le nombre n étant supérieur à 3, a_4 désigne une lettre nouvelle. Le produit de la première substitution par la seconde est

$$(a_3, a_4)(a_1, a_2)$$

et ce produit doit figurer dans le système proposé. Donc celui-ci renferme toutes les substitutions qui équivalent à un nombre pair de transpositions, et son ordre est ainsi au moins égal à $\frac{N}{2}$; d'ailleurs cet ordre est un diviseur de N, par suite il est égal à $\frac{N}{2}$ ou à N.

Le cas de $p>3$ se ramène facilement au cas de $p=3$. En effet, soient a_1, a_2, a_3 trois quelconques des lettres données, et posons

$$T = (a_1, a_2, a_3) = (a_1, a_3)(a_1, a_2).$$

Soit aussi

$$S = (a_1, a_2, b_4, b_5, \ldots, b_p, a_3)$$

une substitution circulaire d'ordre p formée avec les lettres a_1, a_2, a_3 et $p-3$ autres lettres données b_4, $b_5, \ldots, b_p$. On aura

$$(a_1, a_2)S = (a_1)(a_2, b_4, b_5, \ldots, b_p, a_3),$$

et, en multipliant, à gauche, par (a_1, a_3),

$$TS = (a_1, a_3, a_2, b_4, b_5, \ldots, b_p).$$

Par hypothèse le système proposé renferme toutes les substitutions circulaires d'ordre p : donc les substitutions TS et S^{-1} doivent y figurer ainsi que leur produit T, qui est l'une quelconque des substitutions circulaires formées avec trois des lettres données.

Si le nombre p est pair, le système proposé comprend les produits de transpositions, en nombre impair, qui équivalent aux substitutions circulaires d'ordre p ; l'ordre de ce système est donc supérieur à $\frac{N}{2}$, et, en conséquence, il est égal à N.

431. Théorème III. — *Une substitution quelconque* T *étant formée avec n lettres, les diverses substitutions des mêmes lettres qui sont échangeables avec* T *constituent un système conjugué.*

En effet, soient

$$1, S_1, S_2, \ldots, S_{M-1}$$

les M substitutions échangeables avec T, parmi lesquelles figure évidemment l'unité. Nous avons vu que le produit de plusieurs de ces substitutions est lui-même une substitution échangeable avec T ; ce produit fait donc partie de la suite précédente, et, en conséquence, celle-ci forme un

système conjugué d'ordre M. Ce nombre M a pour valeur (nº **414**)

$$M=(1.2\ldots m_1)(1.2\ldots m_2)\ldots(1.2\ldots m_\omega)n_1^{m_1}n_2^{m_2}\ldots n_\omega^{m_\omega},$$

m_i désignant le nombre des cycles de T qui sont de l'ordre n_i. On tient compte des cycles formés d'une seule lettre, en sorte que l'on a

$$n=m_1n_1+m_2n_2+\ldots+m_\omega n_\omega.$$

Ainsi en particulier avec un nombre n de lettres égal à m_1n_1, on peut former, par le précédent théorème, un système conjugué d'ordre

$$1.2.3\ldots m_1\times n_1^{m_1}.$$

Exemple. — Dans le cas de

$$n=6=3\times 2=2\times 3,$$

on pourra former deux systèmes de substitutions conjuguées dont les ordres seront respectivement $1.2.3\times 2^3$ ou 48, et 1.2×3^2 ou 18.

432. Théorème IV. — *Une substitution quelconque* T *étant formée avec n lettres, les diverses substitutions* S *telles, que le produit* STS^{-1} *se réduise à une puissance de* T, *constituent un système de substitutions conjuguées.*

Le nombre des substitutions qui satisfont à l'égalité

$$STS^{-1}=T^i,$$

dans laquelle i représente un nombre donné premier à l'ordre de la substitution T, est égal (nº **421**) au nombre M des substitutions échangeables avec S. Si donc on désigne par ν le nombre des substitutions S qui satisfont à la précédente égalité, lorsque i cesse d'être un nombre donné, et par $\varphi(\mu)$ le nombre qui indique com-

bien il y a de nombres premiers à l'ordre μ de la substitution T, on aura

$$\nu = M\varphi(\mu).$$

Cela posé, soient

$$(1)\qquad 1,\ S_1,\ S_2,\ S_3,\ \ldots,\ S_{\nu-1}$$

les substitutions qui satisfont à la condition imposée par l'énoncé du théorème. Je dis que le produit de deux quelconques des substitutions (1) fait partie de la même suite, et que celle-ci constitue en conséquence un système conjugué d'ordre ν. Considérons, en effet, les deux substitutions S_1, S_2; on a par hypothèse

$$(2)\qquad S_1 T S_1^{-1} = T^j, \quad \text{ou} \quad S_1 T = T^j S_1,$$

$$(3)\qquad S_2 T S_2^{-1} = T^j, \quad \text{ou} \quad S_2 T = T^j S_2;$$

en multipliant à gauche par S_1 l'égalité (3), il vient

$$(4)\qquad S_1 S_2 T = S_1 T^j S_2;$$

et, en élevant l'égalité (2) à la puissance j, on a

$$S_1 T S_1^{-1} . S_1 T S_1^{-1} \ldots S_1 T S_1^{-1} = T^{ij},$$

c'est-à-dire

$$(5)\qquad S_1 T^j S_1^{-1} = T^{ij}, \quad \text{ou} \quad S_1 T^j = T^{ij} S_1;$$

en vertu de cette égalité (5), la formule (4) donne

$$(6)\qquad S_1 S_2 T = T^{ij} S_1 S_2, \quad \text{ou} \quad (S_1 S_2) T (S_1 S_2)^{-1} = T^{ij},$$

d'où il suit que la substitution $S_1 S_2$ fait partie de la suite (1), comme on l'avait annoncé.

433. Soient e l'un des nombres premiers à μ, et θ l'exposant auquel e appartient relativement au module μ. Au lieu de former la suite (1) avec toutes les substitutions S, qui satisfont à l'égalité

$$STS^{-1} = T^i,$$

où i a une valeur quelconque, si l'on prend seulement les substitutions S qui satisfont à la même égalité en imposant la condition que i soit congru, suivant le module μ, à une puissance de e, les substitutions de la suite (1) formeront encore un système conjugué. Effectivement, si l'on suppose que dans les égalités (2) et (3) i et j désignent deux puissances de e, le produit ij sera lui-même une puissance de e, et, en vertu de l'égalité (6), le produit $S_1 S_2$ appartiendra à la suite (1). On peut donc énoncer le théorème suivant :

Théorème V. — *Une substitution quelconque* T, *d'ordre* μ, *étant formée avec n lettres, si l'on forme toutes les substitutions* S *telles, que le produit* STS^{-1} *se réduise à une puissance de* T, *dont l'exposant soit congru, suivant le module* μ, *à une puissance d'un nombre donné e appartenant à l'exposant* θ, *par rapport au module* μ, *les substitutions* S *constitueront un système conjugué d'ordre* θM. *Lorsque le nombre* μ *admet des racines primitives,* θ *peut être un diviseur quelconque de* $\varphi(\mu)$.

Ce théorème V comprend le théorème III comme cas particulier; il se confond avec celui-ci quand on fait $\theta = 1$ et, par suite, $e = 1$. Mais il ne comprend pas le théorème IV, parce qu'il n'existe pas en général de racines primitives pour un nombre composé. Cette extension du théorème III a été indiquée par M. C. Jordan, dans un Mémoire qui fait partie du XXXVIIIe Cahier du *Journal de l'École Polytechnique*.

Corollaire I. — *On peut former, avec n lettres, des systèmes de substitutions conjuguées d'ordre* $n\varphi(n)$ *et d'ordre* $\frac{n\varphi(n)}{t}$, *t étant un diviseur convenable de n. En particulier, si n est un nombre premier, on peut former*

un système de substitutions conjuguées dont l'ordre soit égal à $n(n-1)$ ou au quotient de ce nombre par un diviseur quelconque de $n-1$.

Ce corollaire résulte immédiatement des théorèmes IV et V, en supposant que T y désigne une substitution circulaire d'ordre n.

Corollaire II. — *On peut former, avec $n-1$ lettres données, un système conjugué d'ordre $\varphi(n)$ ou $\frac{\varphi(n)}{t}$.*

Considérons en effet le système conjugué qui contient $n\varphi(n)$ ou $\frac{n\varphi(n)}{t}$ substitutions de n lettres, et dont il est question dans le corollaire précédent. Pour former ce système, on part d'une substitution circulaire T, d'ordre n, et l'on prend les substitutions S qui satisfont à une égalité de la forme $STS^{-1} = T^i$. Or, du mode de formation de ces substitutions S, il résulte que, pour chaque valeur de i, il existe une substitution unique S, qui ne déplace pas une lettre donnée a. Donc le système que nous considérons renferme $\varphi(n)$ ou $\frac{\varphi(n)}{t}$ substitutions qui ne déplacent que $n-1$ lettres; il est évident que ces substitutions constituent un système conjugué.

434. Dans le cas de $n=6$, si l'on choisit d'abord pour T une substitution régulière formée de deux cycles du troisième ordre, on pourra former, par le théorème IV, un système de substitutions conjuguées dont l'ordre sera $1.2\times 3^2\times 2$ ou 36. Si l'on prend en second lieu, pour T, une substitution circulaire du sixième ordre, on pourra former, par le théorème V (corollaire I), un système conjugué d'ordre $6\times\varphi(6)$ ou 12. Soit

$$T = (a, b, c, d, e, f)$$

Corollaire I. — *Si les substitutions* S *et* T *d'ordres respectifs* μ *et* ν *sont échangeables entre elles et n'ont aucune puissance commune autre que l'unité, on formera un système d'ordre* $\mu\nu$ *en multipliant les* μ *puissances de* S *par les* ν *puissances de* T.

En effet, dans l'hypothèse admise, les deux systèmes conjugués

$$1,\ S,\ S^2,\ \ldots,\ S^{\mu-1},$$
$$1,\ T,\ T^2,\ \ldots,\ T^{\nu-1}$$

remplissent les conditions exigées par l'énoncé du théorème précédent.

Corollaire II. — *Si plusieurs substitutions* S, T, U, ..., *d'ordres respectifs* μ, ν, ρ, ..., *sont échangeables entre elles deux à deux, et si l'égalité*

$$S^i T^j U^k \ldots = 1$$

ne peut avoir lieu que pour $i = \mu$, $j = \nu$, $k = \rho$, ..., *on formera un système conjugué d'ordre* $\mu\nu\rho\ldots$ *en multipliant les puissances de* S *par celles de* T, *puis les résultats obtenus par les puissances de* U, *et ainsi de suite.*

Remarque. — Si l'on pose

$$P = (a_0, a_1, \ldots, a_{\rho-1})(b_0, b_1, \ldots, b_{\rho-1})\ldots(f_0, f_1, \ldots, f_{\rho-1}),$$
$$Q = (a_0, b_0, \ldots, f_0)(a_1, b_1, \ldots, f_1)\ldots(a_{\rho-1}, b_{\rho-1}, \ldots, f_{\rho-1}),$$

pour que S et T soient des substitutions échangeables entre elles et que ces substitutions n'aient aucune puissance commune autre que l'unité, il faut et il suffit (n° 417) que l'on ait

$$S = P, \quad T = Q,$$

ou

$$S = PP'P''\ldots, \quad T = QQ'Q''\ldots,$$

P' et Q', P'' et Q'', ... désignant des substitutions formées de la même manière que P et Q, mais avec des lettres différentes.

Considérons, par exemple, le cas de six lettres. Si l'on fait

$$S = (a, b)(c, d)(e, f), \quad T = (a, c)(b, d)(e)(f),$$

on obtiendra un système conjugué du quatrième ordre qui se composera des quatre substitutions

$$1, \; S, \; T, \; ST.$$

436. Examen d'un cas remarquable qui rentre dans les théorèmes V et VI. — Le cas dont il s'agit ici est celui du système de $n(n-1)$ substitutions conjuguées dont il est question dans le corollaire I du théorème V, lorsque le nombre n des lettres est premier.

Soient

$$a_0, \; a_1, \; a_2, \; \ldots, \; a_{n-1}$$

les n lettres données, et supposons, comme au n° 416, que a_{nq+r} désigne la même lettre que a_r. Le système que nous considérons sera formé de toutes les substitutions S qui satisfont à une égalité de la forme

$$STS^{-1} = T^l,$$

dans laquelle T désigne une substitution circulaire d'ordre n. Soit

$$T = (a_0, a_1, a_2, \ldots, a_{n-1})$$

cette substitution. Le nombre n étant premier et i désignant un nombre quelconque non divisible par n, T^i sera une substitution circulaire d'ordre n, et l'on aura, par nos conventions,

$$T^i = [a_0, a_i, a_{2i}, \ldots, a_{(n-1)i}],$$

ou, en faisant passer une lettre quelconque a_{ki} à la pre-

mière place,

$$T^i = [a_{ki}, a_{(k+1)i}, \ldots, a_{(n-1)i}, a_0, a_i, \ldots, a_{(k-1)i}].$$

Cela posé, chaque substitution S doit se former en prenant pour numérateur la permutation qui constitue le cycle de T^i et pour dénominateur la permutation qui figure dans le cycle de T. Désignons par C cette dernière permutation, par C′ et C″ les permutations qui constituent le cycle de T^i lorsqu'on met à la première place a_0 et a_{ki} respectivement. L'expression générale des substitutions S sera

$$S = \begin{pmatrix} C'' \\ C \end{pmatrix} = \begin{pmatrix} C'' \\ C' \end{pmatrix} \begin{pmatrix} C' \\ C \end{pmatrix}.$$

On a évidemment

$$\begin{pmatrix} C'' \\ C' \end{pmatrix} = [a_0, a_{ki}, a_{2ki}, \ldots, a_{(n-1)ki}] = T^{ki};$$

quant à la substitution $\begin{pmatrix} C' \\ C \end{pmatrix}$, elle ne renferme pas la lettre a_0 et l'on a

$$\begin{pmatrix} C' \\ C \end{pmatrix} = \begin{bmatrix} a_i & a_{2i} & \ldots & a_{(n-1)i} \\ a_1 & a_2 & \ldots & a_{n-1} \end{bmatrix}.$$

Cette substitution a pour effet de multiplier par i les indices des lettres a; soit r une racine primitive pour le nombre premier n, posons

$$i \equiv r^\nu \pmod{n},$$

et désignons par U la substitution qui a pour effet de multiplier par r les indices des lettres a : il est clair que la puissance $\nu^{\text{ième}}$ de U multipliera ces indices par r^ν ou i: on aura donc

$$\begin{pmatrix} C' \\ C \end{pmatrix} = U^\nu;$$

on voit en outre, à cause de $r^{n-1} \equiv 1 \pmod{n}$, que U est

une substitution circulaire de l'ordre $n-1$ dont l'expression est

$$U = (a_1, a_r, a_{r^2}, a_{r^3}, \ldots a_{r^{n-2}}).$$

Il résulte de là que, si l'on désigne par h un nombre tel, que l'on ait $h \equiv ki \pmod{n}$, la substitution S aura pour valeur

(1) $$S = T^h U^\nu;$$

enfin, de l'équation

$$STS^{-1} = T^i$$

on tire

$$ST^kS^{-1} = T^{ki} = T^h = SU^{-\nu},$$

d'où

$$T^kS^{-1} = U^{-\nu}$$

et

(2) $$S = U^\nu T^k.$$

Les formules (1) et (2) fourniront donc la même valeur de S, si les exposants h et k satisfont à la relation

$$h = kr^\nu.$$

Chacune de ces mêmes formules donnera toutes les substitutions du système que nous considérons en attribuant à h ou à k les n valeurs $0, 1, 2, \ldots, n-1$, et à ν les mêmes valeurs, zéro excepté, ou, ce qui revient au même, $n-1$ excepté. En d'autres termes, le système dont nous nous occupons s'obtiendra en multipliant les substitutions

$$1, T, T^2, \ldots, T^{n-1},$$

à droite ou à gauche, par les substitutions

$$1, U, U^2, \ldots, U^{n-2}.$$

Exemple. — Considérons le cas de $n = 5$. Comme 2 est ici racine primitive, on pourra former un système de

vingt substitutions conjuguées en multipliant entre elles les puissances des deux substitutions

$$T = (a_0, a_1, a_2, a_3, a_4), \quad U = (a_1, a_2, a_4, a_3);$$

il est facile de vérifier sur cet exemple que la formule

$$U^\nu T^k U^{-\nu} = T^{k.2^\nu}$$

a lieu quels que soient les nombres k et ν.

437. Théorème VII. — *Étant donné un système de n lettres, soient n_1 un nombre entier égal ou inférieur à n, et $\nu = m_1 n_1$ un multiple de n_1 contenu dans n. Soient encore n_2 un nombre égal ou inférieur à m_1, et $m_2 n_2$ un multiple de n_2 contenu dans m_1. Soient pareillement n_3 un nombre égal ou inférieur à m_2, et $m_3 n_3$ un multiple de n_3 contenu dans m_2, ... On pourra toujours, avec ν lettres arbitrairement choisies parmi les n lettres données, former un système de substitutions conjuguées dont l'ordre sera $n_1^{m_1} n_2^{m_2} n_3^{m_3} \ldots$.*

Ce théorème a été démontré par Cauchy, dans le Mémoire que nous avons déjà eu l'occasion de citer.

Prenons $\nu = m_1 n_1$ lettres parmi les n qui sont données, puis distribuons-les en m_1 groupes ou arrangements composés chacun de n_1 lettres, et que nous nommerons groupes de *première espèce*. Prenons ensuite ces m_1 arrangements pour composer les cycles de m_1 substitutions circulaires d'ordre n_1, que nous représenterons par

(1) $$P_1, P_2, P_3, \ldots, P_{m_1}.$$

Parmi les m_1 groupes de première espèce, prenons-en $m_2 n_2$ et distribuons-les en m_2 groupes de *deuxième espèce*, lesquels seront ainsi formés par la réunion de n_2 groupes de première espèce. Avec les $n_1 n_2$ lettres de chaque

groupe de deuxième espèce, formons une substitution ayant pour effet de déplacer circulairement les groupes de première espèce contenus dans le groupe de deuxième espèce, et soient

$$(2)\qquad Q_1,\ Q_2,\ Q_3,\ \ldots,\ Q_{m_2}$$

les m_2 substitutions ainsi obtenues. Si C, C′, C″, ... désignent les arrangements ou groupes de première espèce qui composent un groupe de deuxième espèce, chaque substitution (2) sera de la forme

$$(CC'C''\ldots)\quad \text{ou}\quad \begin{pmatrix} C'C''C''' \ldots \\ C\ C'\ C''\ldots \end{pmatrix};$$

elle a pour effet de remplacer chaque lettre de C par celle qui occupe le même rang dans C′, celle-ci par celle qui occupe le même rang dans C″, et ainsi de suite. Il résulte de là que les substitutions Q sont régulières et que chacune d'elles est formée de n_1 cycles d'ordre n_2.

Parmi les m_2 groupes de deuxième espèce, prenons-en $m_3 n_3$ et distribuons-les en m_3 groupes de *troisième espèce*, lesquels comprendront ainsi n_3 groupes de deuxième espèce. Avec les $n_1 n_2 n_3$ lettres de chaque groupe de troisième espèce, formons une substitution ayant pour effet de déplacer circulairement les groupes de deuxième espèce contenus dans celui de troisième espèce, et soient

$$(3)\qquad R_1,\ R_2,\ R_3,\ \ldots,\ R_{m_3}$$

les m_3 substitutions ainsi obtenues. En reproduisant le raisonnement que nous avons fait à l'égard des substitutions Q, on prouvera que chacune des substitutions R est régulière, et qu'elle est formée de $n_1 n_2$ cycles d'ordre n_3. On peut continuer ainsi tant que l'on n'aura pas rencontré l'unité dans la suite des nombres m_1, m_2, m_3, ...

Dans chacune des suites (1), (2), (3), ..., deux substitutions quelconques n'ont aucune lettre commune, et,

par suite, elles sont échangeables entre elles. On obtiendra donc un système de substitutions conjuguées P d'ordre $n_1^{m_1}$ en multipliant entre elles les m_1 suites qui sont formées chacune par les n_1 puissances de l'une des substitutions (1). Pareillement, on obtiendra de la même manière des systèmes conjugués Q, R, ..., dont les ordres seront respectivement $n_2^{m_2}$, $n_3^{m_3}$, ..., au moyen des substitutions (2), (3), ...

Je dis en outre que deux quelconques des systèmes ainsi formés sont échangeables entre eux. A cet effet, représentons les lettres contenues dans chacun des divers arrangements ou groupes d'une espèce quelconque par un même caractère a ou b, ou c, ... affecté d'un indice variable; alors celles des substitutions P, Q, R, ... qui ont pour effet d'échanger circulairement les groupes d'espèces moins élevées contenues dans l'un des groupes que nous considérons pourront se déduire de celles qui se rapportent à un autre groupe, en changeant la lettre que nous sommes convenus d'affecter d'indices, mais en conservant les mêmes indices. Si donc A et B désignent deux arrangements de $i^{\text{ème}}$ espèce formés respectivement de deux lettres a, b, affectées des mêmes indices, et si l'une des substitutions P, Q, ... change A en A', l'une de ces substitutions changera aussi B en B', les indices de b dans B' se succédant dans le même ordre que les indices de a dans A'.

Cela posé, soit V une substitution de l'une des suites (2), (3), ... qui déplace circulairement les groupes A, B, C, D, ..., K de $i^{\text{ème}}$ espèce, contenus dans un groupe ABCD...L de $(i+1)^{\text{ième}}$ espèce. Soit en même temps U l'une des substitutions (1), (2), (3), ... qui ne produisent de déplacements de lettres que dans l'un des arrangements A, B, ..., dans C par exemple. Supposons que U change C en C'; d'après ce que nous venons de

dire, le système auquel U appartient renfermera une autre substitution U' changeant aussi D en D'. Appliquons successivement les trois substitutions U, V, U'^{-1} à l'arrangement

$$ABCD\ldots K.$$

Par la substitution U, cet arrangement devient d'abord

$$ABC'D\ldots K;$$

il se transforme ensuite en

$$BCD'\ldots KA$$

par la substitution V. Enfin, comme la substitution U'^{-1} change D' en D, elle nous donnera l'arrangement

$$BCD\ldots A,$$

que l'on aurait obtenu tout d'abord en appliquant la substitution V à l'arrangement primitif; on a donc

$$U'^{-1}VU = V, \quad \text{d'où} \quad VU = U'V.$$

Il résulte de là que les systèmes conjugués P, Q, R, ... sont échangeables entre eux deux à deux. D'ailleurs un produit tel que V...RQP, formé avec des substitutions de ces divers systèmes, ne peut se réduire à l'unité à moins que tous ses facteurs ne se réduisent eux-mêmes à l'unité; car, s'il en était autrement, on aurait

$$\ldots RPQ = V^{-1},.$$

ce qui est impossible, puisque la substitution contenue dans le premier membre est impropre à déplacer les groupes de lettres que V^{-1} échange entre eux. On voit donc que l'on obtiendra un système de substitutions conjuguées d'ordre $n_1^{m_1} n_2^{m_2} n_3^{m_3} \ldots$ en multipliant entre eux les systèmes P, Q, R, ...

Corollaire I. — *Étant donné un système de n let-*

439. Théorème VIII. — *Si l'on a formé un système de substitutions conjuguées de m lettres dont l'ordre soit μ, et un système de substitutions conjuguées de p lettres dont l'ordre soit ϖ, on pourra construire un système de substitutions conjuguées de $n = mp$ lettres, dont l'ordre sera $\mu^p \varpi$.*

En effet, distribuons les mp lettres données en p groupes composés chacun de m lettres, et que nous représenterons par

$$\begin{array}{l} a_0,\ a_1,\ a_2,\ \ldots,\ a_{m-1},\\ b_0,\ b_1,\ b_2,\ \ldots,\ b_{m-1},\\ \ldots\ldots\ldots\ldots\ldots\ldots,\\ k_0,\ k_1,\ k_2,\ \ldots,\ k_{m-1}. \end{array}$$

Soit A un système de μ substitutions conjuguées, formées avec les m lettres a qui composent la première ligne de ce tableau. Soient aussi B, C, ..., K les systèmes de substitutions conjuguées que l'on obtient en remplaçant successivement dans A la lettre a par b, c, d, ..., k, sans changer les indices dont la lettre est affectée. Désignons enfin par

$$1,\ S_i,\ T_i,\ \ldots,\ U_i$$

ϖ substitutions conjuguées, formées avec les p lettres a_i, b_i, ..., k_i; posons

$$S = S_0 S_1 \ldots S_{m-1},\quad T = T_0 T_1,\ \ldots,\ T_{m-1},$$

et nommons P le système conjugué d'ordre ϖ

$$1,\ S,\ T,\ \ldots,\ U,$$

dont les substitutions ont pour effet d'échanger entre elles les lignes horizontales de notre tableau.

Les systèmes A, B, ... K sont évidemment échangeables entre eux, et il est aisé de voir que leur produit est échangeable avec le système P. En effet, soient A une

substitution du système A, et S une substitution de P; la substitution A, effectuée la première, déplacera les lettres a et elle remplacera la première ligne du tableau par

$$a'_0,\ a'_1,\ a'_2,\ \ldots,\ a'_{m-1},$$

après quoi la substitution S déplacera les lignes horizontales du tableau; seulement, si elle doit amener les lettres b à la place de a, la ligne précédente sera remplacée par

$$b'_0,\ b'_1,\ b'_2,\ \ldots,\ b'_{m-1},$$

et, pour faire disparaître les accents, il suffira d'appliquer la substitution B^{-1}, B désignant ce que devient A quand on y remplace a par b. On voit alors que l'on a

$$B^{-1}PA = P, \quad \text{d'où} \quad PA = BP.$$

Il résulte évidemment de là qu'en multipliant entre eux les $p+1$ systèmes A, B, C, ..., K et P, on obtiendra un système conjugué dont l'ordre sera $\mu^p \varpi$.

Corollaire I. — *On peut former, avec $n = mp$ lettres, un système de substitutions conjuguées d'ordre* $(1.2.3\ldots m)^p.(1.2\ldots p)$.

Il suffit en effet de prendre pour A le système de toutes les substitutions formées avec m lettres, et pour P le système de toutes les substitutions formées avec p lettres.

Exemples. — Dans le cas de $n = 6$, on peut faire $m = 3$, $p = 2$, ou $p = 2$, $m = 3$. On voit alors que l'on peut former avec six lettres deux systèmes de substitutions conjuguées, dont les ordres sont respectivement 72 et 48. Dans le cas de $n = 4$, on a $m = 2$, $p = 2$, et l'on peut former avec quatre lettres un système conjugué d'ordre 8.

Corollaire II. — *Si p est un nombre premier, on peut former, avec $n = mp$ lettres, un système de substitutions conjuguées d'ordre* $(1.2.3\ldots m)^p\, p(p-1)$.

Il suffit en effet de choisir A comme dans le précédent corollaire, et de prendre pour P le système conjugué d'ordre $p(p-1)$ dont nous avons reconnu l'existence dans le cas où p est un nombre premier. Le système dont il s'agit ici se rencontre dans la théorie des équations.

440. Théorème IX. — *Si un système de substitutions conjuguées relatif à n lettres renferme toutes les substitutions circulaires du troisième ordre que l'on peut former avec $n-1$ lettres données, et qu'il ait encore d'autres substitutions, il renferme toutes les substitutions circulaires du troisième ordre que l'on peut former avec les n lettres.*

Soient

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-2},\ b$$

les n lettres données, G le système que l'on considère, et G′ le système conjugué formé avec celles des substitutions de G qui ne contiennent pas b. Désignons par T une substitution de G qui n'appartienne pas à G′, et supposons que T substitue b, a_i, a_j à a_0, a_1, a_2, i et j étant deux indices quelconques qui peuvent avoir les valeurs 1 et 2; comme la substitution $U=(a_0, a_1, a_2)$ appartient à G, par hypothèse, il en sera de même de $TUT^{-1}=(b, a_i, a_j)$. Le système G renferme donc toutes les substitutions circulaires formées avec les n lettres.

Corollaire. — *Si un système de substitutions conjuguées relatif à n lettres renferme toutes les $1.2.3\ldots(n-1)=\frac{N}{n}$ substitutions formées avec $n-1$ lettres, son ordre est N ou $\frac{N}{n}$. Si le système proposé renferme seulement les $\frac{N}{2n}$ substitutions du premier genre formées avec $n-1$ lettres, son ordre est $\frac{N}{2}$ ou $\frac{N}{2n}$.*

Conservons les notations dont nous venons de faire usage. Par hypothèse, l'ordre de G' est $\frac{N}{n}$ ou $\frac{N}{2n}$; le même nombre exprimera donc aussi l'ordre de G, si ce système n'a que les seules substitutions de G'. Dans le cas contraire, G admettra toutes les substitutions circulaires du troisième ordre formées avec les n lettres, et son ordre sera N ou $\frac{N}{2}$, savoir : N si G' renferme toutes les substitutions de $n-1$ lettres, et $\frac{N}{2}$ si G' renferme seulement des substitutions du premier genre.

441. Théorème X. — *Si un système de substitutions conjuguées relatif à n lettres ne renferme pas toutes les substitutions circulaires du troisième ordre formées avec n — 1 lettres, mais qu'il contienne toutes celles que l'on peut former avec n — 2 des lettres données, les substitutions du système qui déplacent les deux autres lettres ne peuvent que les échanger entre elles. Le nombre n est supposé supérieur à 4.*

Soient

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-3},\ b_0,\ b_1$$

les n lettres données, G le système que l'on considère, et G' le système conjugué formé par celles des substitutions de G qui ne déplacent aucune des lettres b_0, b_1; par hypothèse le système G renferme toutes les substitutions circulaires du troisième ordre que l'on peut former avec les $n-2$ lettres a. Désignons par T une substitution de G qui n'appartienne pas à G' et qui n'échange pas entre elles les lettres b_0 et b_1.

Si T déplace b_0 pour la substituer à a_0 et qu'elle ne déplace pas b_1 ou que, déplaçant b_1, elle la substitue à b_0, soient a_1 et a_2 les deux lettres qui seront remplacées par

deux lettres quelconques données, a_i, a_j; comme la substitution $U=(a_0, a_1, a_2)$ appartient à G, il en est de même de $TUT^{-1}=(b_0, a_i, a_j)$; donc le système G renferme toutes les substitutions circulaires du troisième ordre qu'on peut former avec $n-1$ des lettres données, ce qui est contre l'hypothèse.

Si T substitue b_0 et b_1 à a_0 et a_1, a_i à a_2, la substitution $U=(a_0, a_1, a_2)$ appartenant à G, il en sera de même de $TUT^{-1}=(b_0, b_1, a_i)$. Or cette dernière substitution remplace a_i par b_0, et b_0 par b_1; on rentre donc dans le cas précédent, qui est incompatible avec notre hypothèse, comme on vient de le voir,

Il résulte de là que la substitution T ne peut qu'échanger les lettres b_0, b_1 entre elles; elle sera donc de la forme $T=(b_0, b_1).S$, S étant une substitution de G'. On voit aussi que le système G s'obtiendra en multipliant entre eux le système G' et le système formé des deux substitutions 1, (b_0, b_1). En conséquence, l'ordre du système G est double de l'ordre du système G'.

REMARQUE. — La démonstration précédente exige que le nombre des lettres a soit au moins égal à 3, et que l'on ait en conséquence $n>4$. Le théorème ne subsiste pas pour $n=4$.

COROLLAIRE. — *Si un système de substitutions conjuguées relatif à n lettres renferme les*

$$1.2.3\ldots(n-2)=\frac{N}{n(n-1)}$$

substitutions formées avec $n-2$ des lettres données, mais qu'il ne renferme pas toutes celles qu'on peut former avec $n-1$ lettres, son ordre sera égal au quotient de N par l'un des deux nombres $\frac{n(n-1)}{2}$, $n(n-1)$. Si le sys-

tème renferme seulement les $\frac{N}{2n(n-1)}$ *substitutions du premier genre formées avec* $n-2$ *lettres, mais qu'il ne contienne pas toutes celles que l'on peut former avec* $n-1$ *lettres, son ordre sera égal au quotient de* N *par l'un des deux nombres* $n(n-1)$, $2n(n-1)$.

En effet, par hypothèse, l'ordre de G′ est $\frac{N}{n(n-1)}$ ou $\frac{N}{2n(n-1)}$, et le même nombre exprimera l'ordre de G, si ce système n'a que les seules substitutions de G′. Dans le cas contraire, toute substitution de G qui n'appartient pas à G′ déplace circulairement les deux lettres non contenues dans G′, car autrement G posséderait toutes les substitutions circulaires du troisième ordre qu'on peut former avec $n-1$ lettres, et cela est contre l'hypothèse. Alors, d'après le théorème précédent, l'ordre de G est double de l'ordre de G′.

Des groupes de permutations.

442. Considérons un système Γ de substitutions conjuguées de n lettres, dont l'ordre soit égal à μ; soient

$$1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1}$$

les substitutions de ce système. Si l'on prend une quelconque des permutations des n lettres données, et que l'on multiplie cette permutation A_0 par les μ substitutions de Γ, on obtiendra μ produits

$$A_0,\ S_1A_0,\ S_2A_0,\ \ldots,\ S_{\mu-1}A_0,$$

ou

$$A_0,\ A_1,\ A_2,\ \ldots,\ A_{\mu-1},$$

qui constituent ce qu'on nomme un *groupe de permuta-*

tions. Les substitutions du système Γ, par lesquelles on passe d'une permutation à une autre, sont dites les *substitutions du groupe*.

Désignons par G, soit le système des $N = 1.2.3\ldots n$ substitutions des lettres données, soit tout autre système conjugué contenant toutes les substitutions du système Γ. On a vu au n° 425 que, si l'on désigne par $m = \mu q$ l'ordre du système G, les substitutions de ce système peuvent être représentées de l'une ou de l'autre des deux manières suivantes :

$$(1)\quad \left\{\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ T_1, & S_1T_1, & S_2T_1, & \ldots, & S_{\mu-1}T_1, \\ T_2, & S_1T_2, & S_2T_2, & \ldots, & S_{\mu-1}T_2, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T_{q-1}, & S_1T_{q-1}, & S_2T_{q-1}, & \ldots, & S_{\mu-1}T_{q-1}; \end{array}\right.$$

$$(2)\quad \left\{\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ U_1, & U_1S_1 & U_1S_2, & \ldots, & U_1S_{\mu-1} \\ U_2, & U_2S_1, & U_2S_2, & \ldots, & U_2S_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ U_{q-1}, & U_{q-1}S_1, & U_{q-1}S_2, & \ldots, & U_{q-1}S_{\mu-1}. \end{array}\right.$$

Cela posé, on obtiendra un groupe de m permutations, en multipliant la permutation A_0, prise arbitrairement, par les m substitutions de G ; et, pour effectuer cette opération, on peut supposer à G l'une ou l'autre des formes (1) et (2).

Employons d'abord la forme (1). La première ligne horizontale est formée des μ substitutions du système Γ, et les produits de la permutation A_0 par ces substitutions donneront le groupe déjà considéré plus haut, savoir :

$$A_0,\ A_1,\ A_2,\ \ldots,\ A_{\mu-1}.$$

Pour multiplier A_0 par les substitutions de la deuxième

ligne du tableau (1), il suffit de faire le produit $A_0^{(1)}$ de la permutation A_0 par T_1 et de multiplier ensuite ce produit par les substitutions Γ; les résultats

$$A_0^{(1)},\ A_1^{(1)},\ A_2^{(1)},\ \ldots,\ A_{\mu-1}^{(1)},$$

qu'on obtiendra ainsi, forment évidemment un deuxième groupe de permutations qui admet les mêmes substitutions que le précédent.

Comme ce que nous venons de dire s'applique évidemment à chacune des lignes du tableau (1), à partir de la deuxième, on voit que *le groupe de permutations obtenu en multipliant une permutation* A_0 *par les* μq *substitutions du système* G *est décomposable en* q *groupes formés chacun de* μ *permutations; en outre, ces divers groupes partiels admettent les mêmes substitutions, savoir, celles du système* Γ.

Opérons maintenant de la même manière en employant le système G sous la forme (2). La première ligne du tableau (2) donnera, comme précédemment, le groupe

$$A_0,\ A_1,\ A_2,\ \ldots,\ A_{\mu-1};$$

quant aux lignes suivantes du tableau (2), elles donneront pour résultats les produits obtenus en multipliant successivement ce premier groupe de permutations par les substitutions

$$U_1,\ U_2,\ \ldots,\ U_{q-1},$$

et, comme ces opérations équivalent à de simples changements dans la notation employée pour désigner les lettres, chacune d'elles transformera le premier groupe en un autre groupe. Il résulte de là que *le groupe obtenu en multipliant la permutation* A_0 par *les* μq *substitutions du système* G *est décomposable en* q *groupes de* μ *permutations tels, qu'on passe d'un groupe à un autre en*

exécutant une même substitution sur les permutations du premier.

Il peut arriver que les lignes horizontales soient les mêmes dans les deux tableaux (1) et (2). Cette circonstance se présentera nécessairement si les substitutions

$$1, T_1, T_2, \ldots, T_{q-1},$$

ou

$$1, U_1, U_2, \ldots, U_{q-1}$$

forment un système conjugué échangeable avec le système Γ. Dans ce cas, *le groupe de permutations obtenu en multipliant la permutation* A_0 *par les* μq *substitutions du système G est décomposable en q groupes formés chacun de* μ *permutations et qui jouissent de cette double propriété, que les substitutions sont les mêmes dans les divers groupes partiels et qu'on passe de l'un de ces groupes à un autre en exécutant une même substitution sur les permutations du premier.*

443. Exemple. — Considérons le cas de quatre lettres a, b, c, d, et prenons les quatre systèmes de substitutions conjuguées

$$\begin{aligned}
G &= 1,\ (a, b)(c, d),\\
G' &= 1,\ (a, c)(b, d),\\
G'' &= 1,\ (b, c, d),\ (b, d, c),\\
G''' &= 1,\ (b, c).
\end{aligned}$$

Les systèmes G et G' sont échangeables, et leur produit G'G, qui est du quatrième ordre, est un système conjugué échangeable avec G''; enfin le système conjugué G''G'G est lui-même échangeable avec G''', en sorte que le produit G'''G''G'G comprend les vingt-quatre substitutions.

Cela posé, multiplions la permutation *abcd* par le sy-

tème $G'''G''G'G$, nous obtiendrons le groupe des vingt-quatre permutations, savoir :

abcd	*acdb*	*adbc*	*acbd*	*abdc*	*adcb*
badc	*cabd*	*dacb*	*cadb*	*bacd*	*dabc*
cdab	*dbac*	*bcad*	*bdac*	*dcab*	*cbad*
dcba	*bdac*	*cbda*	*dbca*	*cdba*	*bcda*

Ce groupe se décompose en deux autres ; l'un de ceux-ci comprend les permutations des trois premières colonnes, et il admet, comme le second, les douze substitutions du premier genre ; on passe de l'un des groupes partiels à l'autre en exécutant la transposition (b, c).

Le premier de ces deux groupes se décompose lui-même en trois autres, formés chacun des permutations contenues dans une même colonne ; ici les trois groupes partiels admettent les quatre substitutions du système $G'G$, et l'on passe d'un groupe à un autre en exécutant une même substitution de G''.

Enfin le premier de ces trois derniers groupes est décomposable en deux autres qui sont formés, l'un des deux premières permutations, l'autre des deux dernières. Ici chacun des groupes partiels admet la substitution de G, et on passe de l'un à l'autre groupe en exécutant la substitution de G'.

CHAPITRE III.

DES INDICES DES SYSTÈMES CONJUGUÉS.

Indice d'un système conjugué.—Limite inférieure des indices supérieurs à 2.

444. Pour abréger le discours, je nommerai *indice* d'un système de substitutions conjuguées formées avec n lettres le quotient obtenu en divisant le produit $N = 1.2.3 \ldots n$ par le nombre qui exprime l'ordre du système. Si m désigne l'indice d'un système conjugué d'ordre μ, on aura

$$m = \frac{N}{\mu};$$

l'ordre et l'indice d'un système conjugué relatif à n lettres sont donc deux diviseurs *correspondants* du produit $1.2.3 \ldots n$.

L'indice m peut avoir les valeurs 1 et 2, quel que soit le nombre n des lettres, et il serait intéressant de connaître en général les plus petites valeurs qu'il peut avoir quand il est supérieur à 2.

Rufini, dans sa théorie des équations, a considéré particulièrement le cas de cinq lettres, et l'on peut conclure de ses recherches que :

Dans le cas des cinq lettres, si l'indice d'un système conjugué est supérieur à 2, *il est au moins égal à* 5.

Cauchy, dans un Mémoire qui fait partie du Xe Cahier du *Journal de l'École Polytechnique*, a démontré en-

suite un théorème plus général duquel il résulte que :

L'indice d'un système de substitutions conjuguées, formées avec n lettres, ne peut être en même temps supérieur à 2 et inférieur au plus grand des nombres premiers qui ne surpassent pas n.

Et, dans le cas où n est un nombre premier, on a ce théorème :

L'indice d'un système de substitutions conjuguées, formées avec n lettres, n étant un nombre premier, ne peut être en même temps supérieur à 2 et inférieur à n.

Cauchy donne à entendre, dans son Mémoire, qu'il chercha à étendre le précédent théorème au cas où n est un nombre composé, mais il ne put d'abord y parvenir que dans le cas de $n = 6$. Il a, en effet, démontré que :

L'indice d'un système de substitutions conjuguées, formées avec six lettres, ne peut être en même temps supérieur à 2 et inférieur à 6.

M. Bertrand s'est occupé ensuite avec succès de cette même question, et il est parvenu à démontrer généralement, et pour la première fois, que :

L'indice d'un système de substitutions conjuguées, formées avec n lettres, ne peut être en même temps supérieur à 2 et inférieur à n (*).

Toutefois la démonstration de M. Bertrand repose sur un postulatum qui semble absolument étranger à la théorie, et, à ce point de vue, elle n'est pas complétement satisfaisante. Le postulatum dont il s'agit a été démontré au n° 403, et il consiste en ce que :

Si l'on a $n > 7$, il y a au moins un nombre premier compris entre $\frac{n}{2}$ et $n - 2$.

(*) *Journal de l'École Polytechnique*, XXXe Cahier.

Le raisonnement dont M. Bertrand a fait usage conduit à cet autre théorème démontré auparavant par Abel, dans le cas de $n = 5$.

Si l'indice d'un système de substitutions conjuguées, formées avec n lettres, est égal à n, le système conjugué se compose des $1.2\ldots(n-1)$ *substitutions de* $n-1$ *lettres.*

Dans une Note qui fait partie du XXXIIe Cahier du *Journal de l'École Polytechnique,* j'ai fait voir que si, entre $n-2$ et $\frac{n}{2}$, il n'y a aucun nombre premier, le théorème de M. Bertrand subsiste, pourvu que $\frac{n}{2}$ soit un nombre premier. La démonstration n'est en aucune façon modifiée; seulement on ne peut plus conclure ce corollaire, que, si l'indice d'un système conjugué est égal au nombre n des lettres, le système est formé par les $1.2\ldots(n-1)$ substitutions de $n-1$ lettres.

Cette remarque a quelque importance, car il en résulte que le théorème de M. Bertrand comprend celui de Cauchy pour le cas de $n = 6$, et rend, par suite, inutile la démonstration un peu compliquée qui se rapporte à ce cas particulier. En effet, si $n = 6$, il n'y a aucun nombre premier entre $n-2$ et $\frac{n}{2}$; mais $\frac{n}{2}$ ou 3 est un nombre premier.

M. Bertrand a démontré aussi, dans son Mémoire, le théorème suivant :

Si l'indice d'un système de substitutions conjuguées, formées avec n lettres, n étant > 9, *est supérieur à n, cet indice est au moins égal à* $2n$.

Plus tard, dans un Mémoire que j'ai présenté à l'Académie des Sciences, en 1849, j'ai démontré, sans avoir

recours à aucun postulatum, les théorèmes suivants (*) :

1° *L'indice d'un système de substitutions conjuguées, formées avec n lettres, ne peut être en même temps supérieur à 2 et inférieur à n, à moins que n ne soit égal à 4.*

2° *Si l'indice d'un système conjugué est précisément égal au nombre n des lettres, le système est formé de toutes les substitutions de n — 1 lettres, à moins que n ne soit égal à 6.*

3° *Si l'indice d'un système conjugué est supérieur au nombre n des lettres, il est au moins égal à 2n, pourvu que n soit > 8.*

4° *Si l'indice d'un système conjugué, relatif à n lettres, est supérieur à 2n, il est au moins égal à* $\frac{n(n-1)}{2}$, *pourvu que n soit > 12.*

Les démonstrations que j'ai données de ces propositions ne laissent rien à désirer sous le rapport de la rigueur. Cauchy, de son côté, avait repris la question et il avait obtenu d'autres démonstrations des mêmes théorèmes; ces démonstrations reposent sur des notions nouvelles qui ont une grande importance dans la théorie dont nous nous occupons, et que nous ne pouvons passer sous silence. Mais nous croyons devoir rappeler d'abord les considérations dont l'illustre géomètre a fait usage, dans son premier Mémoire, pour établir la première des propositions énoncées dans cet aperçu, ainsi que l'analyse ingénieuse et élégante par laquelle M. Bertrand est parvenu à démontrer son théorème.

445. Théorème de Cauchy. — *L'indice d'un système de substitutions conjuguées, formées avec n lettres,*

(*) *Journal de Mathématiques pures et appliquées*, 1re série, t. XV.

ne peut être en même temps supérieur à 2 et inférieur au plus grand des nombres premiers qui ne surpassent pas n.

En effet, considérons un système G d'ordre μ de substitutions conjuguées formées avec n lettres, et soient

$$1,\ S_1,\ S_2,\ S_3,\ \ldots,\ S_{\mu-1}$$

ces substitutions. Si on les multiplie à gauche, pour fixer les idées, par les diverses puissances d'une substitution circulaire quelconque T, dont l'ordre p soit un nombre premier égal ou inférieur à n, on formera le tableau suivant :

$$\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ T, & TS_1, & TS_2, & \ldots, & TS_{\mu-1}, \\ T^2, & T^2S_1, & T^2S_2, & \ldots, & T^2S_{\mu-1}, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots, \\ T^{p-1}, & T^{p-1}S_1, & T^{p-1}S_2, & \ldots, & T^{p-1}S_{\mu-1}, \end{array}$$

qui comprendra μp substitutions. Si l'indice $\frac{N}{\mu}$ du système G est inférieur à p, on aura $\mu p > N$, et, en conséquence, on trouvera nécessairement deux substitutions égales dans le tableau précédent. Soit donc

$$T^\alpha S_i = T^\beta S_j;$$

les exposants α et β doivent être supposés inégaux, car, si l'on avait $\beta = \alpha$, il s'ensuivrait $S_j = S_i$ ou $j = i$. De l'égalité précédente on tire

$$T^{\alpha-\beta} = S_j S_i^{-1} \quad \text{ou} \quad T^\gamma = S_j S_i^{-1};$$

le produit $S_j S_i^{-1}$ étant une substitution du système G, distincte de l'unité, on voit que ce système renferme néces-

sairement une puissance T^γ de T ; il contient donc toutes les puissances de T^γ. Mais l'ordre de la substitution circulaire T étant un nombre premier, cette substitution fait partie de la suite des puissances de T^γ, et en conséquence elle appartient au système G.

Le système G renferme donc toutes les substitutions circulaires d'ordre p, et il s'ensuit (n° 430) qu'il comprend N ou $\frac{N}{2}$ substitutions; en d'autres termes, son indice est égal à 1 ou à 2.

446. Théorème de M. Bertrand. — *L'indice d'un système de substitutions conjuguées, formées avec n lettres, ne peut être en même temps supérieur à 2 et inférieur à n.*

Ainsi que nous l'avons déjà dit, M. Bertrand admet ce postulatum : *Si n est > 7, il y a au moins un nombre premier compris entre $\frac{n}{2}$ et $n - 2$.*

Cela posé, considérons un système G composé des substitutions conjuguées

$$1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1},$$

formées avec n lettres, et supposons que l'indice $\frac{N}{\mu}$ de ce système soit inférieur à n. Désignons par p un nombre premier compris entre $\frac{n}{2}$ et $n - 2$, et prenons arbitrairement $p + 2$ lettres parmi les n lettres données; formons avec p de ces $p + 2$ lettres une substitution circulaire T d'ordre p, et avec les deux lettres restantes une transposition U. Cela posé, multiplions les substitutions du système G à gauche, par exemple, par les p puissances de T, puis les produits obtenus par les deux puissances de U;

on formera de cette manière les deux tableaux :

$$\begin{cases} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ T, & TS_1, & TS_2, & \ldots, & TS_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T^{p-1}, & T^{p-1}S_1, & T^{p-1}S_2, & \ldots, & T^{p-1}S_{\mu-1}, \end{cases}$$

$$\begin{cases} U, & US_1, & US_2, & \ldots, & US_{\mu-1}, \\ UT, & UTS_1, & UTS_2, & \ldots, & UTS_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ UT^{p-1}, & UT^{p-1}S_1, & UT^{p-1}S_2, & \ldots, & UT^{p-1}S_{\mu-1}, \end{cases}$$

dans lesquels on trouve $2p\mu$ substitutions. Mais, par hypothèse, p est au moins égal à $\frac{n}{2}$ et μ est lui-même supérieur à $\frac{N}{n}$; donc le nombre de nos substitutions surpasse N, et, en conséquence, il est nécessaire que deux d'entre elles soient égales.

Si ces deux substitutions égales appartiennent au même tableau, on aura, par exemple,

$$T^\alpha S_i = T^6 S_j, \quad \text{ou} \quad UT^\alpha S_i = UT^6 S_j,$$

α et 6 étant deux exposants inégaux, et il en résultera

$$T^{\alpha-6} = S_j S_i^{-1};$$

la substitution $T^{\alpha-6}$ appartient donc au système G, et l'on en conclut, comme dans le précédent théorème, que la substitution T fait elle-même partie de ce système.

Si les deux substitutions égales n'appartiennent pas au même tableau, on aura

$$T^\alpha S_i = UT^6 S_j = T^6 U S_j,$$

car on peut intervertir l'ordre des substitutions U et T

qui n'ont pas de lettres communes. De cette égalité on tire, à cause de $U^{-1} = U$,

$$T^{\alpha-\beta}U = S_j S_i^{-1},$$

d'où il résulte que la substitution $T^{\alpha-\beta}U$ appartient au système G, et il en est de même du carré

$$T^{2\alpha-2\beta}U^2 = T^{2\alpha-2\beta}$$

de cette substitution. La différence $\alpha - \beta$ peut être nulle, et alors la substitution U appartient au système G; si $\alpha - \beta$ n'est pas nulle, la substitution $T^{2(\alpha-\beta)}$ appartient au système G, ainsi que toutes ses puissances, parmi lesquelles figure T, comme dans l'hypothèse précédente. Dans ce dernier cas, T et $T^{\alpha-\beta}U$ appartiennent au système G, il en est de même de U.

On voit en résumé que l'une au moins des deux substitutions T et U appartient au système G.

Supposons maintenant que l'indice du système proposé ne se réduise pas à 1, ou que l'ordre de ce système ne soit pas égal à N. Alors, parmi les transpositions que l'on peut former avec les n lettres données, il y en aura au moins une qui ne fera pas partie des substitutions du système G; nous prendrons pour U cette transposition, et, d'après ce qui vient d'être établi, toute substitution circulaire T d'ordre p, formée avec celles des $n-2$ lettres données qui ne figurent pas dans U, appartiendra au système G. Celles des substitutions de G qui ne déplacent pas les deux lettres de la transposition U forment évidemment un système conjugué G′, et, puisque ce système G′ renferme toutes les substitutions circulaires d'ordre p, son ordre est égal à $1.2.3\ldots(n-2)$ ou à la moitié de ce nombre (n° 430). Mais le premier cas ne peut avoir lieu, car autrement, l'indice de G étant supérieur à 1,

cet indice serait au moins égal à n (n° **441**, *Corollaire*), ce qui est contre l'hypothèse. Donc l'ordre de G′ est $\frac{1.2\ldots(n-2)}{2}$, et, par suite, l'indice de ce système est égal à 2.

Le système G′ n'a ainsi que des substitutions du premier genre, et, en conséquence, le système G ne renferme aucune des transpositions que l'on peut former avec les lettres relatives à G′. Désignons par U′ l'une quelconque de ces transpositions et par T′ une substitution circulaire d'ordre p qui ne contienne aucune des lettres de U′, mais qui, au contraire, renferme les deux lettres de U, ou au moins l'une d'elles. Comme la transposition U′ ne se trouve pas dans G, la substitution T′ appartiendra à ce système, comme on l'a vu plus haut, d'où il suit que le système G renferme toutes les substitutions circulaires d'ordre p que l'on peut former avec les n lettres données; il contient donc les $\frac{N}{2}$ substitutions du premier genre que l'on peut former avec ces lettres. Il est évident d'ailleurs que le système G ne peut renfermer d'autres substitutions puisqu'il ne possède pas les substitutions du deuxième genre formées avec les $n-2$ lettres relatives à G′; donc l'ordre de ce système est égal à $\frac{N}{2}$ et son indice est égal à 2 (*).

447. La démonstration précédente subsiste quand il n'existe pas de nombre premier entre $\frac{n}{2}$ et $n-2$, pourvu

(*) On aurait pu tirer immédiatement cette conclusion des propositions établies aux n°s 440 et 441; mais il nous a paru convenable de conserver dans son intégrité le raisonnement par lequel M. Bertrand a établi son théorème.

que $\frac{n}{2}$ soit un nombre premier; dans ce cas, on peut poser $p = \frac{n}{2}$; tel est le cas de $n = 6$. Mais, quand il existe un nombre premier p effectivement compris entre $\frac{n}{2}$ et $n - 2$, le raisonnement que nous avons développé peut servir à démontrer une proposition nouvelle fort importante. Effectivement, pour établir que le système G possède l'une au moins des substitutions T et U, il n'est pas nécessaire de supposer, comme nous l'avons fait, que l'indice de G soit inférieur à n; la même chose a lieu encore quand cet indice est égal à n, pourvu que l'on ait $p > \frac{n}{2}$, et l'on arrive toujours à cette conséquence que l'indice de G' est 1 ou 2. Cet indice ne peut être égal à 2, car il en résulterait, comme on l'a vu, que l'indice de G serait lui-même égal à 2, ce qui est contre l'hypothèse; l'indice de G' est donc égal à 1; mais alors (n° **441**, *Corollaire*) l'indice de G ne peut pas être égal à n, à moins que ce système ne soit formé par les substitutions de $n - 1$ lettres. De là résulte le théorème suivant :

Théorème. — *Si l'indice d'un système de substitutions conjuguées est égal au nombre n des lettres, le système se compose des* $1.2.3\ldots(n-1)$ *substitutions formées avec n — 1 lettres.*

La démonstration ne s'applique pas aux cas de $n = 3, 4, 5, 6, 7$. Le théorème a été démontré par Abel pour $n = 5$ (*OEuvres complètes*, t. I[er], p. 19), et il a lieu aussi pour les cas de $n = 4, 5, 7$, comme on le verra plus loin. Le seul cas de $n = 6$ fait exception; nous établirons qu'il existe effectivement un système de substitutions conjuguées de 6 lettres dont l'indice est égal à 6 et qui renferme des substitutions circulaires des ordres 4, 5, 6.

Démonstration nouvelle du théorème relatif à la limite inférieure des indices plus grands que 2.

448. Je vais faire connaître actuellement la démonstration par laquelle je suis parvenu à établir directement le théorème de M. Bertrand; j'ai publié cette démonstration pour la première fois dans le tome XV du *Journal de Mathématiques pures et appliquées* (1re série), et je l'ai reproduite dans la précédente édition de cet Ouvrage. Mais, en la présentant ici, je profiterai des secours que m'offrent les propositions établies dans le Chapitre précédent, ce qui me permettra d'apporter quelques simplifications; la démonstration dont il s'agit sera fondée sur deux lemmes que nous établirons d'abord.

Lemme I. — *Soient* G *un système de substitutions conjuguées formées avec n lettres* $a_0, a_1, a_2, \ldots, a_{n-3}, b_0, b_1$, *et* G' *le système conjugué formé avec celles des substitutions de* G *qui ne déplacent aucune des deux lettres* b_0, b_1. *Si les systèmes* G *et* G' *ont un même indice* μ *supérieur à* 1, *on pourra construire avec les* $n-2$ *lettres* $a_0, a_1, \ldots, a_{n-3}$ *un système de substitutions conjuguées dont l'indice sera* $\frac{\mu}{2}$; *d'où il suit que le nombre* μ *est toujours pair.*

Désignons par ν et ρ les ordres respectifs des systèmes G et G'. Les indices de ces systèmes seront $\frac{1.2.3\ldots n}{\nu}$ et $\frac{1.2.3\ldots(n-2)}{\rho}$; comme ils sont égaux, par hypothèse, on aura

$$\nu = n(n-1)\rho.$$

Posons

$$G = 1,\ S_1,\ S_2,\ S_3,\ \ldots,\ S_{\rho-1},\ \ldots,\ S_{\nu-1},$$
$$G' = 1,\ S_1,\ S_2,\ S_3,\ \ldots,\ S_{\rho-1}.$$

Si l'on représente par $T_1, T_2, \ldots, T_{\mu-1}$ des substitutions des $n-2$ lettres a, le système des $\mu\rho = 1.2.3\ldots(n-2)$ substitutions des $n-2$ lettres a pourra (n° 425) être représenté par

$$(1)\quad \left\{\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\rho-1}, \\ T_1, & T_1 S_1, & T_1 S_2, & \ldots, & T_1 S_{\rho-1}, \\ T_2, & T_2 S_1, & T_2 S_2, & \ldots, & T_2 S_{\rho-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T_{\mu-1}, & T_{\mu-1} S_1, & T_{\mu-1} S_2, & \ldots, & T_{\mu-1} S_{\rho-1}; \end{array}\right.$$

et je dis que le système des $\mu\nu = 1.2\ldots n$ substitutions des n lettres est compris dans le nouveau tableau

$$(2)\quad \left\{\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\nu-1}, \\ T_1, & T_1 S_1, & T_1 S_2, & \ldots, & T_1 S_{\nu-1}, \\ T_2, & T_2 S_1, & T_2 S_2, & \ldots, & T_2 S_{\nu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T_{\mu-1}, & T_{\mu-1} S_1, & T_{\mu-1} S_2, & \ldots, & T_{\mu-1} S_{\nu-1}, \end{array}\right.$$

où les substitutions T sont les mêmes que dans le tableau (1). Il suffit de prouver que ces $\mu\nu$ substitutions sont distinctes. Si l'on avait

$$T_i S_j = T_{i'} S_{j'},$$

on en conclurait

$$T_{i'} = T_i S_j S_{j'}^{-1};$$

or les facteurs T sont indépendants de b_0 et b_1, donc le produit $S_j S_{j'}^{-1}$, qui est l'une des substitutions S_k du système G, ne contient pas b_0 et b_1 ; il en résulte que S_k fait partie du système G'. D'ailleurs l'égalité précédente devient

$$T_{i'} = T_i S_k,$$

ce qui n'est pas possible, d'après la manière dont les substitutions T ont été choisies pour former le tableau (1).

Le tableau (2) renferme donc toutes les substitutions des n lettres; or, si l'on applique ces substitutions à une permutation quelconque, il y en aura évidemment $1.2.3\ldots(n-2)$ qui transporteront deux lettres quelconques données à deux places déterminées; d'ailleurs, les substitutions T ne contenant pas b_0 et b_1, il est évident que toutes les μ substitutions contenues dans une même colonne verticale du tableau (2) donneront à b_0 et à b_1 les mêmes places; il y aura donc, dans la première ligne horizontale du tableau, c'est-à-dire dans le système G, $\frac{1.2.3\ldots(n-2)}{\mu}$ ou ρ substitutions qui transporteront b_0 et b_1 à deux places quelconques et qui, en conséquence, substitueront ces lettres, dans la permutation primitive, à deux lettres quelconques, parmi lesquelles b_0 et b_1 peuvent se trouver; en particulier il y aura *précisément* ρ substitutions qui échangeront b_0 et b_1 entre elles. Si l'on pose

$$U = (b_0, b_1),$$

ces ρ substitutions seront de la forme

$$US'_0,\ US'_1,\ US'_2,\ \ldots,\ US'_{\rho-1},$$

$S'_0, S'_1, \ldots, S'_{\rho-1}$ étant des substitutions indépendantes de b_0 et de b_1. Aucune de ces substitutions S′ ne peut se réduire à l'unité, ou plus généralement à l'une des substitutions du système G′; car, si S'_i appartenait à G′, et par suite à G, comme US'_i est aussi une substitution de G, il en serait de même de U. Je dis que cela ne peut être; en effet, on a vu que les substitutions S_i de G peuvent substituer b_0 et b_1 à deux lettres quelconques, et inversement substituer deux lettres quelconques à b_0 et b_1; d'après cela, si U appartenait à G, il en serait de même de toutes les substitutions de la forme $S_i U S_i^{-1}$, c'est-à-dire de

toutes les transpositions; l'indice de G serait alors égal à 1, ce qui est contre l'hypothèse.

Cela posé, prenons dans le système G les ρ substitutions de G' avec les ρ précédentes, il est évident que les 2ρ substitutions obtenues, savoir :

$$(3)\quad \begin{cases} 1, & S_1, & S_2, & \ldots, & S_{\rho-1}, \\ US'_0, & US'_1, & US'_2, & \ldots, & US'_{\rho-1}, \end{cases}$$

formeront un système conjugué. En effet, les produits $S_i S_j$ et $US'_i \times US'_j = S'_i S'_j$ appartiennent à G, et, comme ils sont indépendants de b_0 et de b_1, ils font partie de la première ligne du tableau (3); pareillement le produit $S_i \times US'_j = U \times S_i S'_j$, appartenant à G, fait nécessairement partie de la seconde ligne du tableau (3). On peut conclure de là que les substitutions

$$(4)\quad \begin{cases} 1, & S_1, & S_2, & \ldots, & S_{\rho-1}, \\ S'_0, & S'_1, & S'_2, & \ldots, & S'_{\rho-1} \end{cases}$$

forment un système de 2ρ substitutions conjuguées de $n-2$ lettres; l'indice de ce système est égal à $\frac{\mu}{2}$, comme on l'avait annoncé.

449. Lemme II. — *Soient* G *un système de substitutions conjuguées, formées avec n lettres* $a_0, a_1, a_2, \ldots, a_{n-m-1}, b_0, b_1, \ldots, b_{m-1}$, *et* G' *le système composé de celles des substitutions de* G *qui ne déplacent aucune des m lettres b. L'indice de* G *ne peut être inférieur à l'indice* μ *de* G', *et, si on le représente par* $\mu + \lambda$, *on pourra former un système* G_1 *de substitutions conjuguées de* $n - m$ *lettres, dont l'indice* μ_1 *sera égal ou inférieur à* λ, *et dont toutes les substitutions seront contenues dans le système* G.

tiplie ses substitutions par λ substitutions

$$1,\ U_1,\ U_2,\ \ldots,\ U_{\lambda-1}$$

convenablement choisies, les produits obtenus

$$(3)\quad \left\{\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\nu-1}, \\ U, & U_1 S_1, & U_1 S_2, & \ldots, & U_1 S_{\nu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ U_{\lambda-1}, & U_{\lambda-1} S_1, & U_{\lambda-1} S_2, & \ldots, & U_{\lambda-1} S_{\nu-1} \end{array}\right.$$

comprendront les $1.2.3\ldots(n-m)$ substitutions qui ne déplacent pas m certaines lettres; je désignerai par $b'_0, b'_1, \ldots, b'_{m-1}$ ces m lettres, et par $a'_0, a'_1, \ldots, a'_{n-m-1}$ les $n-m$ autres. Soient

$$G_1 = 1,\ S'_1,\ S'_2,\ \ldots,\ S'_{\rho_1-1}$$

les ρ_1 substitutions de G qui ne déplacent pas les m lettres b', on obtiendra le système de toutes les

$$1.2.3\ldots(n-m)$$

substitutions des lettres a', en multipliant G_1 par certaines substitutions indépendantes des lettres b', qui feront évidemment partie des facteurs $1, U_1, U_2, \ldots, U_{\lambda-1}$, et que l'on peut représenter par

$$1,\ U_1,\ U_2,\ \ldots,\ U_{\mu_1-1};$$

alors on aura

$$\mu_1 \rho_1 = 1.2.3\ldots(n-m),$$

et le nombre μ_1, égal ou inférieur à λ, exprimera l'indice du système G_1 dont toutes les substitutions sont contenues dans G.

430. Ces lemmes établis, nous passons à la démonstration des théorèmes que nous avons en vue.

THÉORÈME I. — *Le nombre n étant impair, si l'indice d'un système de substitutions conjuguées, formées avec n lettres, est plus grand que 2, cet indice est égal ou supérieur à n; et, quand il est égal à n, le système conjugué est composé de toutes les substitutions que l'on peut former avec n — 1 lettres.*

Le théorème est évident dans le cas de $n = 3$; car, l'indice du système étant supérieur à 2, il est nécessairement égal ou supérieur à 3. En outre, si cet indice est égal à 3, l'ordre du système est $\frac{1.2.3}{3}$ ou 2, qui est un nombre premier. Le système est alors formé des deux puissances d'une substitution circulaire du deuxième ordre, c'est-à-dire d'une transposition.

Il résulte de là que, pour établir le théorème énoncé dans toute sa généralité, il suffit de prouver que, s'il a lieu pour $n = n'$, il subsiste aussi pour $n = n' + 2$. En d'autres termes, nous pouvons admettre que le théorème a lieu quand on remplace, dans son énoncé, n par $n - 2$, le nombre n étant un nombre impair, au moins égal à 5.

Soient G le système conjugué donné dont nous supposons l'indice supérieur à 2, et G' le système conjugué composé de celles des substitutions de G qui ne déplacent pas deux lettres choisies arbitrairement parmi les n lettres données. D'après ce que nous admettons, l'indice de G' ne peut être en même temps supérieur à 2 et inférieur à $n - 2$; cet indice sera donc l'un des cinq nombres

$$1,\ 2,\ n-2,\ n-1,\ n,$$

ou bien il sera supérieur à n, auquel cas l'indice de G sera lui-même plus grand que n. Nous allons examiner successivement ces cinq hypothèses.

1° *L'indice de* G' *est* 1. — Comme, par hypothèse, l'indice de G n'est pas 1, cet indice est égal (nos 440 et 441,

Corollaires) à l'un des nombres n, $\frac{n(n-1)}{2}$, $n(n-1)$, et en outre, si cet indice est égal à n, le système G est composé de toutes les substitutions de $n-1$ lettres.

2° *L'indice de* G' *est* 2. — Dans ce cas, l'indice de G, qu'on suppose différent de 2, est l'un des nombres $2n$, $n(n-1)$, $2n(n-1)$ (n°s 440 et 441); il est donc supérieur à n.

3° *L'indice* G' *est* $n-2$. — Dans ce cas, l'indice de G ne peut être égal à $n-2$, d'après le lemme I (n° 448), parce que $n-2$ est un nombre impair. Si l'indice de G est égal à $n-1$ ou à n, on pourra former, d'après le lemme II (n° 449), un système conjugué de substitutions de $n-2$ lettres, dont l'indice sera 1 ou 2 et dont toutes les substitutions seront contenues dans G; on rentre donc dans l'une des deux hypothèses précédentes, quand l'indice de G n'est pas supérieur à n.

4° *L'indice de* G' *est* $n-1$. — Dans ce cas, l'indice de G ne peut être $n-1$; car, si cet indice était $n-1$, on pourrait former, d'après le lemme I, un système conjugué de substitutions de $n-2$ lettres, dont l'indice serait $\frac{n-1}{2}$. Or, si n est >5, le nombre $\frac{n-1}{2}$ est supérieur à 2 et il est inférieur à $n-2$; nous admettons d'ailleurs que l'indice d'un système conjugué relatif à $n-2$ lettres ne peut être en même temps supérieur à 2 et inférieur à $n-2$; donc l'hypothèse que nous discutons en ce moment est inadmissible quand n est supérieur à 5. Mais elle l'est aussi lorsque $n=5$, car dans ce cas l'indice de G' ne peut pas être supposé égal à $n-1=4$, puisque 4 n'est pas un diviseur du produit $1.2.3$.

L'indice de G, s'il n'est pas supérieur à n, est donc égal à n; mais alors, d'après le lemme II, on pourra former

un système conjugué de substitutions de $n-2$ lettres, ayant 1 pour indice et dont toutes les substitutions seront contenues dans G. On rentre ainsi dans la première des hypothèses que nous venons d'examiner.

5° *L'indice de* G′ *est n.* — Dans ce cas, l'indice de G est nécessairement supérieur à n; car, d'après le lemme I, cet indice ne peut être égal à n, puisque n est un nombre impair.

On conclut de là que l'indice de G supposé plus grand que 2 ne peut être en aucun cas inférieur à n, et que si cet indice est égal à n, le système G est formé par les substitutions de $n-1$ lettres.

451. Théorème II. — *Le nombre n étant pair, si l'indice d'un système de substitutions conjuguées formées avec n lettres est plus grand que 2, cet indice est égal ou supérieur à n, le cas de $n=4$ étant excepté. Et, si l'indice du système est précisément égal à n, celui-ci est composé de toutes les substitutions formées avec $n-1$ lettres, le seul cas de $n=6$ étant excepté.*

Soient G le système conjugué donné, et G_0 le système conjugué formé par celles des substitutions de G qui ne déplacent pas une lettre choisie arbitrairement parmi les lettres données. Nous supposons que l'indice de G est supérieur à 2; quant à l'indice de G_0 qui se rapporte à $n-1$ lettres seulement, il ne peut, d'après ce qui précède, être en même temps supérieur à 2 et inférieur à $n-1$, puisque $n-1$ est un nombre impair. Cet indice de G_0 sera donc l'un des nombres

$$1,\ 2,\ n-1,\ n,$$

ou bien il sera supérieur à n, et, dans ce cas, l'indice de G sera lui-même plus grand que n. Nous allons examiner les quatre hypothèses précédentes :

1° *L'indice de* G_0 *est* 1. — Dans ce cas, l'indice de G est égal à n (n° 440, *Corollaire*), puisqu'on suppose cet indice différent de 1.

2° *L'indice de* G_0 *est* 2. — Dans ce cas, l'indice de G est égal à $2n$ (n° 440), puisqu'on le suppose différent de 2.

3° *L'indice de* G_0 *est* $n-1$. — Dans ce cas, comme $n-1$ est impair, le système G_0 (n° 450) est formé par toutes les substitutions de $n-2$ lettres, et son indice, qui est plus grand que 1, est égal (n°s 440 et 441) à l'un des nombres n, $\frac{n(n-1)}{2}$, $n(n-1)$, pourvu cependant que n soit > 4 [1]. En outre, cet indice ne peut être égal à n que dans le cas où G renferme toutes les substitutions de $n-1$ lettres.

4° *L'indice de* G_0 *est* n. — Alors l'indice de G est égal ou supérieur à n; il nous reste à examiner le cas où cet indice est précisément égal à n.

Remarquons d'abord que la première partie du théorème énoncé se trouve établie par ce qui précède, savoir: *Si le nombre pair* n *est supérieur à* 4, *l'indice d'un système conjugué, relatif à* n *lettres, ne peut être à la fois supérieur à* 2 *et inférieur à* n. Dans ce qui va suivre, nous supposerons $n-2>4$, et, par suite, $n>6$. Désignons par G' le système conjugué formé par celles des substitutions de G_0 qui ne déplacent pas l'une des $n-1$ lettres relatives à G_0, lettre qui peut d'ailleurs être choisie à volonté. L'indice de G' ne peut être à la fois supérieur à 2 et inférieur à $n-2$, d'ailleurs il n'est pas supérieur à n; donc il a pour valeur l'un des cinq

(¹) Nous avons vu (n° 439) qu'on peut former avec quatre lettres un système de substitutions conjuguées dont l'ordre est 8 et dont l'indice est conséquemment égal à 3.

nombres 1, 2, $n-2$, $n-1$, n. Le cas où cet indice serait l'un des nombres $n-2$, $n-1$ se ramène immédiatement, par le lemme II, au cas où il serait 1 ou 2; or je dis que ce dernier cas ne peut avoir lieu; car, si l'indice de G' est 1 ou 2, l'indice de G_0 sera nécessairement l'un des nombres 1, 2, $(n-1)$, $2(n-1)$ (n° 440) dont aucun ne peut être égal à n. L'indice de G' est donc égal à n; mais alors, d'après le lemme I, on pourrait former un système conjugué de substitutions de $n-2$ lettres, dont l'indice serait $\frac{n}{2}$, ce qui est impossible, puisque l'on a

$$2 < \frac{n}{2} < n-2.$$

Donc notre dernière hypothèse est inadmissible, si le nombre n est supérieur à 6. Elle peut au contraire avoir lieu quand $n=6$, ainsi que nous allons l'établir; mais elle est impossible quand $n=4$, puisque, 4 n'étant pas un diviseur du produit $1.2.3$, l'indice de G_0 ne peut pas être égal à 4. Ainsi le cas de $n=6$ constitue la seule exception à la deuxième partie de notre théorème.

Du système conjugué d'indice 6 qui comprend 120 substitutions de six lettres, et qui n'est pas formé par les 120 substitutions de cinq lettres.

452. Il résulte de la démonstration précédente que, si un tel système existe, celles de ses substitutions qui ne déplacent pas deux lettres quelconques forment un système conjugué de substitutions de quatre lettres, dont l'indice est 6, et dont l'ordre est, en conséquence, $\frac{1.2.3.4}{6}$ ou 4. Ce système d'ordre 4 ne peut renfermer, outre l'unité, que des substitutions circulaires du qua-

trième ordre, des substitutions régulières du deuxième ordre formées de deux cycles, ou des transpositions. Mais il ne saurait y avoir de transpositions, car le système entier des substitutions des six lettres n'en saurait contenir, comme on l'a vu dans la démonstration du lemme du n° 448, lemme qui embrasse le cas que nous considérons ici. Si le système d'ordre 4 dont il est question n'est pas composé des quatre puissances d'une substitution circulaire du quatrième ordre, il comprendra, outre l'unité, les trois substitutions régulières que l'on peut former avec les quatre lettres; donc on y trouvera, dans tous les cas, une substitution régulière formée de deux transpositions. Et, comme il y a quinze combinaisons de six lettres quatre à quatre, le système conjugué G dont nous nous occupons doit comprendre quinze substitutions régulières formées chacune de deux transpositions. Or deux substitutions de cette espèce qui auraient un cycle commun et une troisième lettre commune ne peuvent figurer dans G, car le produit de deux telles substitutions est évidemment une substitution circulaire du troisième ordre; donc, si l'on distribue les quinze transpositions des six lettres en cinq groupes de trois transpositions, de telle manière que les six lettres figurent dans les trois transpositions d'un même groupe, on obtiendra les quinze substitutions régulières de G, en faisant les produits deux à deux des transpositions contenues dans un même groupe. Toute autre substitution régulière de la même espèce a nécessairement un cycle commun et une troisième lettre commune avec l'une des quinze dont nous venons de parler, et par conséquent elle ne peut pas être contenue dans G; ainsi ce système ne renferme pas les trois substitutions régulières formées avec les quatre mêmes lettres, et, par suite, il contient une substitution circulaire de ces quatre lettres.

Soient

$$a,\ b,\ c,\ d,\ e,\ f$$

les lettres données, et supposons que le système G renferme les puissances de la substitution circulaire

$$U = (a,\ b,\ c,\ d).$$

Le même système doit renfermer une substitution circulaire U_1, formée avec les quatre lettres a, b, c, e; on peut supposer que a soit mis au premier rang dans U_1; mais alors c ne pourra occuper la troisième place, car, si cela avait lieu, le produit des deux substitutions régulières U^2 et U_1^2, qui auraient un facteur (a, c) commun, ne contiendrait que deux transpositions ayant une lettre commune b, et il se réduirait à une substitution circulaire du troisième ordre, laquelle ne peut figurer dans G. Il faut donc que c occupe dans U_1 la deuxième ou la quatrième place, et alors il occupera dans U_1^3 la quatrième ou la deuxième. J'appellerai U_1 celle de ces deux substitutions dans laquelle c occupe la quatrième place: on aura donc

$$U_1 = (a,\ b,\ e,\ c) \quad \text{ou} \quad U_1 = (a,\ e,\ b,\ c);$$

pareillement, le système G renferme deux substitutions circulaires du quatrième ordre dont chacune est le cube de l'autre, et qui sont formées avec les quatre lettres a, b, c, f; je désignerai par U_2 celle de ces substitutions dans laquelle c occupe la deuxième place, et l'on aura

$$U_2 = (a,\ c,\ f,\ b) \quad \text{ou} \quad U_2 = (a,\ c,\ b,\ f).$$

Mais, si l'on prend la première valeur de U_1, il faudra prendre la deuxième valeur de U_2, et inversement, car autrement U_1^2 et U_2^2 auraient une transposition commune, et leur produit se réduirait à une substitution circulaire du troisième ordre. Rien ne distinguant jusqu'ici les let-

tres e et f, nous ferons

$$U_1 = (a, b, e, c), \quad U_2 = (a, c, b, f).$$

Cela posé, en appliquant successivement les substitutions U, U_1, U_2 à une permutation quelconque, on trouve

$$U_1 U = (a, e, c, d, b),$$
$$U_2 U_1 U = (a, e, b, c, d, f).$$

On voit donc que le système G renferme les trois substitutions circulaires

$$U = (a, b, c, d), \quad T = (a, e, c, d, b), \quad S = (a, e, b, c, d, f)$$

des ordres respectifs 4, 5, 6; ce système s'obtiendra donc en multipliant à droite ou à gauche, mais toujours de la même manière, les puissances de U par celles de T, puis les résultats obtenus par celles de S. En opérant ainsi, on formera bien $6 \times 5 \times 4$ ou 120 substitutions distinctes, car il est évident que deux produits, tels que $S^k T^j U^i$, $S^{k'} T^{j'} U^{i'}$, ne peuvent être égaux, à moins que l'on n'ait $k' = k$, $j' = j$, $i' = i$. Mais il reste à faire voir que ces 120 substitutions constituent réellement un système conjugué.

En premier lieu, les systèmes conjugués formés l'un avec les puissances de U, l'autre avec les puissances de T, sont échangeables entre eux. On a effectivement

$$UTU^{-1} = T^2, \quad U^2TU^{-2} = T^4, \quad U^3TU^{-3} = T^3 = T^8,$$

c'est-à-dire

$$U^\nu T U^{-\nu} = T^{2^\nu},$$

et, en élevant à la puissance μ,

$$U^\nu T^\mu U^{-\nu} = T^{\mu \cdot 2^\nu}, \quad \text{d'où} \quad U^\nu T^\mu = T^{\mu \cdot 2^\nu} U^\nu;$$

ces deux systèmes fournissent donc, par la multiplication, un système conjugué de 20 substitutions relatives à cinq

lettres; en mettant a_0, a_1, a_2, a_3, a_4 au lieu de e, c, d, b, a, on ferait coïncider ce système avec celui que nous avons rencontré au n° 436.

En second lieu, le système conjugué

$$1,\ P_1,\ P_2,\ \ldots,\ P_{19},$$

dont nous venons de parler, est échangeable avec le système conjugué formé par les puissances de S. D'abord, il est facile de vérifier que, quel que soit n, on peut trouver un entier m tel, que chacune des substitutions

$$S^m T S^n,\quad S^m U S^n$$

se réduise à l'une des substitutions P. Le nombre m se détermine facilement par la condition que les substitutions que nous venons d'écrire ne contiennent pas la lettre f, et l'on trouve

$$\begin{array}{l|l}
S^4TS = T^2U = UT, & S^3US = T^4U = UT^2, \\
S^2TS^2 = T^4, & S^4US^2 = T^3U^3 = U^3T, \\
S^5TS^3 = U^2, & S^2US^3 = T^3U^2 = U^2T^2, \\
STS^4 = T^4U^3 = U^3T^3, & SUS^4 = T^4U^2 = U^2T, \\
S^3TS^5 = T^2U^2 = U^2T^3. & S^5US^5 = U^3.
\end{array}$$

On a donc, quel que soit n,

$$S^m TS^n = P_i,\quad S^m US^n = P_i,$$

ou

$$TS^n = S^{-m}P_i,\quad US^n = S^{-m}P_i,$$

m et i ayant des valeurs convenables. Il résulte de là que tout produit de la forme $P_j S^\nu$ peut être ramené à la forme $S^\mu P_k$; en effet, P_j est un produit composé de facteurs T et de facteurs U, et, d'après ce qui précède, on peut faire avancer successivement S^ν d'un rang vers la gauche, en modifiant chaque fois convenablement l'expo-

sant ν; après avoir répété cette opération plusieurs fois, il est clair que $P_j S^\nu$ se trouvera remplacé par une expression de la forme $S^\mu P_k$. Le système des substitutions P et celui des puissances de S étant échangeables entre eux, on obtiendra, en les multipliant l'un par l'autre, un système conjugué d'ordre $24 \times 5 = 120$ ou d'indice 6.

Il importe de remarquer aussi que le système dont nous venons de prouver l'existence comprend des substitutions du premier genre et des substitutions du deuxième genre en nombre égal. En conséquence, les substitutions du premier genre constitueront un système conjugué d'ordre 60 et dont l'indice sera égal à 12.

Des systèmes transitifs de substitutions conjuguées.

453. Lorsque les substitutions d'un système conjugué permettent de substituer successivement l'une des lettres à chacune des autres, le système est dit *transitif*. Il est *intransitif* dans le cas contraire. Cette distinction des systèmes conjugués en transitifs et intransitifs est due à Cauchy; elle a une très-grande importance dans la théorie qui nous occupe.

Plus généralement, si les substitutions d'un système conjugué permettent de substituer m des lettres données à m lettres quelconques, nous dirons que le système est m fois transitif.

Si un système de substitutions conjuguées est m fois transitif, les substitutions du système permettent de substituer m lettres *quelconques* à m lettres quelconques. En effet, le système proposé étant supposé m fois transitif, il y a m lettres $a_1, a_2, \ldots, a_m$ qu'on peut substituer à m autres quelconques $b_1, b_2, \ldots, b_m$, distinctes ou non des premières. Réciproquement, les substitutions du système permettent de remplacer $a_1, a_2, \ldots, a_m$ par b_1,

$b_2, \ldots, b_m$, et, en conséquence, elles peuvent substituer ces dernières lettres à m lettres quelconques.

Il est évident que le système de toutes les substitutions formées avec n lettres est $n-1$ fois transitif, et que le système qui comprend toutes les substitutions du premier genre formées avec les mêmes lettres est $n-2$ fois transitif.

On voit aussi qu'un système de substitutions conjuguées formées avec n lettres est transitif, quand il renferme une substitution circulaire d'ordre n; mais cette condition n'est pas nécessaire. En général, un système conjugué de substitutions de n lettres est m fois transitif, quand il renferme m substitutions circulaires des ordres respectifs $n, n-1, \ldots, n-m+1$. Par exemple, le système d'indice 6, dont nous nous sommes occupé au n° 452 et qui est composé de 120 substitutions conjuguées de six lettres, est trois fois transitif, car il admet trois substitutions circulaires des ordres respectifs 6, 5, 4.

454. Théorème I. — *L'ordre d'un système m fois transitif, de substitutions conjuguées de n lettres, est un multiple de* $n(n-1)\ldots(n-m+1)$; *en d'autres termes, l'indice du système est un diviseur du produit*

$$1.2.3\ldots(n-m).$$

En effet, soient $A_0, A_1, A_2, \ldots$ les $n(n-1)\ldots(n-m+1)$ arrangements m à m que l'on peut former avec les n lettres données, et

$$S_0,\ S_1,\ S_2,\ \ldots,\ S_{\rho-1}$$

celles des substitutions du système proposé G qui remplacent les lettres de l'arrangement A_i par celles qui occupent respectivement les mêmes rangs dans A_j. Désignons, en outre, par T l'une des substitutions de G qui

remplacent les lettres de A_j par celles de A_k, il est clair que les ρ substitutions

$$TS_0, TS_1, TS_2, \ldots, TS_{\rho-1}$$

remplaceront les lettres de A_i par celles de A_k. Le nombre des substitutions qui remplacent A_i par A_k ne peut donc être moindre que le nombre de celles qui remplacent A_i par A_j, et réciproquement ce dernier nombre ne peut être inférieur au premier.

Il résulte de là qu'il y a, dans le système proposé, un même nombre ρ de substitutions qui remplacent l'arrangement donné A_i par chacun des arrangements A_0, A_1, A_2, ... Si donc on appelle μ l'ordre du système G, on aura

$$\mu = n(n-1)\ldots(n-m+1)\times\rho,$$

et l'indice du système sera

$$\frac{N}{\mu} = \frac{1.2.3\ldots n}{\mu} = \frac{1.2.3\ldots(n-m)}{\rho}.$$

Cet indice est, en conséquence, un diviseur du produit $1.2.3\ldots(n-m)$ et l'on voit en outre qu'il est égal à l'indice du système conjugué formé par les ρ substitutions qui remplacent l'un des arrangements A_i par lui-même. De là résulte la proposition suivante :

COROLLAIRE. — *Si un système* G *de substitutions conjuguées est* m *fois transitif, celles des substitutions de* G *qui laissent immobiles* m *lettres choisies à volonté forment un système conjugué* G' *dont l'indice est égal à l'indice de* G.

455. THÉORÈME II. — *Un système de substitutions conjuguées dont l'indice est supérieur à 2 ne peut être* m *fois transitif, s'il renferme une substitution qui ne dé-*

place que i lettres, le nombre i étant supposé égal ou inférieur à m.

En effet, supposons que le système proposé G renferme une substitution S qui ne déplace que i lettres; le nombre m étant au moins égal à i, et le système G étant m fois transitif, ce système renferme une substitution T qui remplace les i lettres contenues dans S par i lettres choisies arbitrairement; par conséquent, il renferme aussi la substitution TST^{-1}, qui est une substitution quelconque semblable à S.

La substitution S étant décomposée en cycles, soit

$$S = CC_1C_2, \ \ldots,$$

et formons la substitution semblable

$$S' = C'C_1^{-1}C_2^{-1}\ldots,$$

le produit

$$S'S = C'C$$

appartiendra au système G. Si l'ordre μ du cycle C est supérieur à 2 et que l'on ait

$$C = (a_0, a_1, a_2, \ \ldots, \ a_{\mu-2}, \ a_{\mu-1}),$$

nous ferons

$$C' = (a_0, a_{\mu-1}, a_{\mu-2}, a_{\mu-3}, \ \ldots, \ a_4, a_3, a_1, a_2)$$

et nous aurons

$$SS' = (a_0, a_2, a_1).$$

Le cas de $\mu = 3$ est compris dans ce qui précède: on a alors $C' = C$; mais, si $\mu = 2$ et que l'on ait

$$C = (a_0, a_1),$$

comme il y a au moins une lettre a_2 non contenue dans S, nous ferons

$$C' = (a_1, a_2),$$

et nous aurons encore

$$SS' = (a_0, a_2, a_1).$$

Ainsi, dans tous les cas, G renferme une substitution circulaire du troisième ordre; donc, si m est égal ou supérieur à 3, G renferme toutes les substitutions circulaires de troisième ordre, et en conséquence son indice est égal à 1 ou 2 (n° 430).

Le cas de $m = 2$ échappe à cette analyse; mais, dans ce cas, le système G contient par hypothèse une des transpositions formées avec les lettres données; donc il les renferme toutes et son indice est égal à 1.

COROLLAIRE. — *Un système de substitutions conjuguées doublement transitif, dont l'indice est supérieur à 2, ne renferme aucune transposition; pareillement, un système triplement transitif, dont l'indice est supérieur à 2, ne renferme aucune transposition et aucune substitution circulaire de trois lettres.*

436. THÉORÈME III. — *Si l'indice d'un système m fois transitif de substitutions conjuguées formées avec n lettres est supérieur à 2, cet indice est un multiple du produit $1.2.3\ldots m$.*

En effet, soient

$$A_0, A_1, A_2, \ldots, A_M$$

les

$$M = 1.2.3\ldots m$$

permutations formées avec m des lettres données choisies arbitrairement, et

$$1, T_1, T_2, \ldots, T_{M-1}$$

les M substitutions de ces mêmes lettres. Soient aussi

$$1, S_1, S_2, \ldots, S_{\varrho-1}$$

celles des substitutions du système proposé G qui ne déplacent pas les m lettres que nous venons de choisir, et qui, en conséquence, remplacent l'arrangement A_0 par lui-même. Il y a dans le système G, comme on l'a vu dans la démonstration du théorème I (nº 454), ρ substitutions susceptibles de remplacer les m lettres de A_0 par celles qui occupent les mêmes rangs dans A_i; mais, pour exécuter une telle substitution, il suffit évidemment de faire d'abord une substitution du système T qui amènera les m lettres de A_i aux places voulues, après quoi il restera seulement à exécuter une substitution S' de $n - m$ lettres. D'ailleurs, les deux substitutions que nous employons sont échangeables entre elles, puisqu'elles n'ont pas de lettres communes, et les ρM substitutions, distinctes du système G, qui sont susceptibles de remplacer l'un des arrangements A par un autre arrangement formé des mêmes lettres, peuvent être représentées par

$$\begin{array}{llll}
1, & S_1, & S_2, \ldots, & S_{\rho-1}, \\
T_1 S_0^{(1)}, & T_1 S_1^{(1)}, & T_1 S_2^{(1)}, \ldots, & T_1 S_{\rho-1}^{(1)}, \\
T_2 S_0^{(2)}, & T_2 S_1^{(2)}, & T_2 S_2^{(2)}, \ldots, & T_2 S_{\rho-1}^{(2)}, \\
\ldots & \ldots & \ldots & \ldots, \\
T_{M-1} S_0^{(M-1)}, & T_{M-1} S_1^{(M-1)}, & \ldots, & T_{M-1} S_{\rho-1}^{(M-1)},
\end{array}$$

où $S_i^{(j)}$ désigne généralement des substitutions qui ne dépendent pas des m lettres contenues dans les arrangements A. Le produit de deux quelconques de ces substitutions appartient au système G ; d'ailleurs il est de la forme $T_i S'$, S' étant indépendant des m lettres contenues dans A ; donc il fait nécessairement partie du tableau précédent ; il en résulte que les $M\rho$ substitutions de ce tableau forment un système conjugué. On voit en outre que les substitutions S, qui figurent comme facteurs

dans deux substitutions de ce système, ne peuvent être égales entre elles; en effet, il est évident que, si $j = i$, on ne peut trouver dans notre tableau les deux substitutions $T_j S$ et $T_i S$, et la même chose a lieu si j est différent de i, car autrement on trouverait aussi $(T_j S)(T_i S)^{-1}$ ou $T_j T_i^{-1}$, ce qui est impossible d'après le théorème II (n° 455), puisque cette substitution ne déplace que m lettres au plus. En conséquence, les $M\rho$ facteurs S du précédent tableau, savoir :

$$\begin{array}{lllll}
1, & S_1, & S_2, & \ldots, & S_{\rho-1}, \\
S_0^{(1)}, & S_1^{(1)}, & S_2^{(1)}, & \ldots, & S_{\rho-1}^{(1)}, \\
S_0^{(2)}, & S_1^{(2)}, & S_2^{(2)}, & \ldots, & S_{\rho-1}^{(2)}, \\
\ldots & \ldots & \ldots & \ldots & \ldots, \\
S_0^{(M-1)}, & S_1^{(M-1)}, & S_2^{(M-1)}, & \ldots, & S_{\rho-1}^{(M-1)},
\end{array}$$

constituent un système de $M\rho$ substitutions conjuguées formées avec $n - m$ lettres; l'ordre $M\rho$ de ce système est donc un diviseur du produit $1.2.3\ldots(n-m)$, et l'on a

$$\frac{1.2.3\ldots(n-m)}{\rho} = k(1.2\ldots m).$$

Or, par le théorème I (n° 456), le premier membre de cette égalité est précisément l'indice du système G : cet indice est donc un multiple de $1.2\ldots m$.

Remarque. — Le théorème que nous venons d'établir comprend, comme cas particulier, la proposition que nous avons présentée au n° 448 à titre de lemme. On peut effectivement conclure de ce qui précède le corollaire suivant :

Corollaire. — *Si un système de substitutions conjuguées formées avec n lettres est m fois transitif, et que*

l'indice μ de ce système soit supérieur à 2, on peut former un système de substitutions conjuguées de $n-m$ lettres dont l'indice est $\frac{\mu}{1.2.3\ldots m}$.

457. Théorème IV. — *Un système de substitutions conjuguées de n lettres, dont l'indice est supérieur à 2, ne peut être plus de $\frac{n}{2}$ fois transitif* (¹).

En effet, quand l'indice μ d'un système m fois transitif de substitutions formées avec n lettres est supérieur à 2, cet indice est en même temps un multiple de $1.2\ldots m$ et un diviseur de $1.2.3\ldots(n-m)$. On ne peut donc pas avoir

$$m > n - m \quad \text{ou} \quad m > \frac{n}{2}.$$

On peut même ajouter que : *Si n est supérieur à 6, il n'existe point de système de substitutions conjuguées formées avec n lettres dont l'indice soit supérieur à 2, et qui soit $\frac{n}{2}$ fois transitif.*

En effet, si un tel système existe, désignons-le par G et soit T l'une de ses substitutions. Supposons que la substitution T remplace les $\frac{n}{2}$ lettres

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_{\frac{n}{2}-2},\ a_{\frac{n}{2}-1}$$

par

$$a'_0,\ a'_1,\ a'_2,\ \ldots,\ a'_{\frac{n}{2}-2},\ a''_{\frac{n}{2}-1};$$

(¹) Ce théorème a été démontré par M. Émile Mathieu dans un Mémoire qui fait partie du tome V du *Journal de Mathématiques pures et appliquées* (2ᵉ série); M. Mathieu a également démontré le théorème II dans ce Mémoire.

le système G renferme une substitution U qui remplace ces $\frac{n}{2}$ dernières lettres par

$$a_0, a_1, a_2, \ldots, a_{\frac{n}{2}-2}, b,$$

b étant une lettre différente des $\frac{n}{2}$ lettres a dont est formé le premier arrangement; la substitution $UT = S$ ne se réduit pas à l'unité et elle ne déplace pas les lettres $a_0, a_1, \ldots, a_{\frac{n}{2}-2}$; donc le système G renferme une substitution qui ne déplace que $\frac{n}{2}+1$ lettres.

Décomposons cette substitution S en cycles, et soit

$$S = CC_1 C_2 \ldots;$$

si T désigne une substitution quelconque de G, $TST^{-1} = S'$ sera une substitution de G semblable à S; posons

$$S' = C' C'_1 C'_2, \ldots.$$

Comme S et S′ ne renferment que $\frac{n}{2}+1$ lettres, on peut choisir T de manière que l'on ait

$$C'_1 = C_1^{-1}, \quad C'_2 = C_2^{-1}, \ldots;$$

on aura alors

$$SS' = CC'.$$

La substitution SS′ appartient à G, et l'on peut même choisir à volonté les lettres de C′, à l'exception d'une seule. Supposons que l'on ait

$$C = (a_0, a_1, a_2, \ldots, a_{i-1}).$$

Si $i = 2$, C se réduit à (a_0, a_1), C′ sera de la forme (b_0, b_1), en choisissant l'une des lettres b_0, b_1 parmi celles qui

ne figurent pas dans S ; la substitution SS' ne déplaçant au plus que quatre lettres, on a nécessairement (n° 455)

$$\frac{n}{2} \overline{\overline{<}} 3 \quad \text{ou} \quad n \overline{\overline{<}} 6.$$

Si i est > 2, on peut faire

$$C' = (a_0, b, a_{i-1}, a_{i-2}, \ldots, a_2);$$

on n'est pas libre du choix de b ; si cette lettre diffère de a_1, le produit SS' ou CC' est $(a_0, b)(a_1, a_2)$, et l'on conclut, comme précédemment, que n est au plus égal à 6. Si la lettre b n'est autre que a_1, on a

$$SS' = (a_0, a_2, a_1),$$

ce qui ne peut avoir lieu que dans le cas de $n = 4$, où l'indice du système deux fois transitif est 2.

Des expressions susceptibles de représenter l'indice d'un système intransitif.

458. Soient G un système intransitif de substitutions conjuguées de n lettres, et

$$a_1, a_2, \ldots, a_\alpha$$

les α lettres que a_1 peut remplacer par les substitutions de G. Si a_i et a_j désignent deux quelconques de ces lettres, le système G renfermera deux substitutions telles que

$$\begin{pmatrix} a_i \ldots \\ a_1 \ldots \end{pmatrix}, \quad \begin{pmatrix} a_j \ldots \\ a_1 \ldots \end{pmatrix};$$

or le produit de la deuxième substitution par l'inverse de la première a pour effet de remplacer la lettre a_j par a_i : donc les substitutions de G peuvent transporter l'une quelconque des lettres a à la place d'une autre lettre quelconque du même groupe. Réciproquement, toute lettre susceptible de remplacer une lettre a_j par les substi-

tutions de G appartient au même groupe; car, si la lettre a peut remplacer a_j, par une substitution de G, cette substitution, combinée avec l'une des précédentes, permettra de remplacer a par a_1 et, conséquemment, la lettre a fait partie du groupe considéré.

Soit b_1 l'une des lettres données non comprises dans le groupe précédent; le raisonnement que nous venons de faire prouve que b_1 fait partie d'un deuxième groupe de lettres

$$b_1,\ b_2,\ \ldots,\ b_6,$$

qui ne peuvent que s'échanger entre elles par les substitutions de G, et, en continuant ainsi, on voit que les n lettres données peuvent être partagées en divers groupes

$$\begin{array}{l} a_1,\ a_2,\ \ldots,\ a_\alpha, \\ b_1,\ b_2,\ \ldots,\ b_6, \\ c_1,\ c_2,\ \ldots,\ c_\gamma, \\ \ldots\ldots\ldots\ldots\ldots, \end{array}$$

de telle manière que les substitutions de G ne puissent qu'échanger entre elles les lettres de chaque groupe. En d'autres termes, chaque substitution S de G sera de la forme

$$S = A.B.C\ldots,$$

A, B, C, ... étant des substitutions qui ne déplacent respectivement que des lettres a, des lettres b, des lettres c, etc.

Il est évident que les substitutions A forment un système transitif relatif à α lettres, et de même les substitutions B, C, ... forment des systèmes transitifs relatifs à 6 lettres, à γ lettres, etc. Désignons par $\mathcal{A}$ l'indice du système conjugué formé des substitutions A, et par $\mathcal{G}$ l'indice du système G.

Il peut arriver que les substitutions A soient en même

nombre que les substitutions de G, et, dans ce cas, on aura

$$\frac{1.2.3\ldots n}{\mathcal{G}} = \frac{1.2\ldots\alpha}{\mathcal{A}},$$

d'où

$$(1) \qquad \mathcal{G} = \frac{1.2.3\ldots n}{1.2.3\ldots\alpha}\mathcal{A}.$$

Mais, si l'ordre μ du système A est inférieur à l'ordre ν de G, il y aura nécessairement dans ce dernier système des substitutions telles que AT, AT′, composées d'une même substitution A et de deux substitutions T, T′ indépendantes des lettres a, ... Le produit de l'une de ces substitutions par l'inverse de l'autre ne déplace pas les lettres a et, en conséquence, le système G renferme un certain nombre ρ de substitutions

$$1, \; T_1, \; T_2, \; \ldots, \; T_{\rho-1},$$

qui ne dépendent pas des lettres a et qui forment un système conjugué que nous désignerons par G′. Maintenant, soit A_1T' l'une des substitutions de G qui renferment le facteur A_1, ce système contiendra les ρ substitutions

$$A_1T', \; A_1T'T_1, \; A_1T'T_2, \; \ldots, \; A_1T'T_{\rho-1},$$

mais il ne contiendra aucune autre substitution renfermant le facteur A_1; car une telle substitution peut se mettre sous la forme $A_1T'\Theta$, et, si elle figurait dans G, Θ y figurerait aussi. Comme A_1 désigne l'une quelconque des $\mu - 1$ substitutions du système A, distinctes de l'unité, on voit que G contient $\mu\rho$ substitutions; ainsi l'on a $\nu = \mu\rho$, ou, en désignant par $\mathcal{G}'$ l'ordre du système G′,

$$\frac{1.2.3\ldots n}{\mathcal{G}} = \frac{1.2.3\ldots\alpha}{\mathcal{A}} \times \frac{1.2.3\ldots(n-\alpha)}{\mathcal{G}'},$$

ce qui donne

$$(2) \qquad \mathcal{G} = \frac{1.2.3\ldots n}{(1.2\ldots\alpha)[1.2\ldots(n-\alpha)]}\,\mathcal{A}\mathcal{G}'.$$

Si l'on suppose que le système G' se réduise à la seule substitution égale à 1, on aura

$$\mathcal{G}' = 1.2.3\ldots(n-\alpha),$$

en sorte que l'on peut regarder la formule (1) comme comprise dans la formule (2).

On peut raisonner sur le système G' comme nous l'avons fait sur le système G, et l'on aura en conséquence

$$\mathcal{G}' = \frac{1.2.3\ldots(n-\alpha)}{(1.2.3\ldots6)[1.2\ldots(n-\alpha-6)]}\,\mathcal{B}\mathcal{G}'',$$

$\mathcal{B}$ étant l'indice d'un système transitif relatif à 6 lettres, et $\mathcal{G}''$ l'indice d'un système relatif à $n-\alpha-6$ lettres.

On peut continuer ainsi jusqu'à ce qu'on rencontre dans la série G, G', G'', ... un système conjugué qui ne soit plus intransitif et qui se rapportera alors au dernier des groupes de lettres données; les formules précédentes donneront

$$(3) \qquad \mathcal{G} = \mathcal{N}\mathcal{A}\mathcal{B}\mathcal{C}\ldots,$$

en posant

$$\mathcal{N} = \frac{1.2.3\ldots n}{(1.2.3\ldots\alpha)(1.2.3\ldots6)(1.2.3\ldots\gamma)\ldots},$$

avec

$$n = \alpha + 6 + \gamma + \ldots.$$

La formule (3), qui a été indiquée par Cauchy, nous fait connaître l'expression des nombres susceptibles de représenter les indices des systèmes intransitifs.

459. Il faut remarquer que la formule (2) peut s'écrire

$$\mathcal{G} = \frac{n(n-1)\ldots(n-\alpha+1)}{1.2\ldots\alpha}\mathcal{A}\mathcal{G}',$$

et, comme α ne peut avoir que les valeurs $1, 2, \ldots, (n-1)$, le premier facteur de cette expression de $\mathcal{G}$ est l'un des nombres

$$\frac{n}{1}, \quad \frac{n(n-1)}{1.2}, \quad \ldots,$$

dont le minimum est n. D'ailleurs $\mathcal{A}$ et $\mathcal{G}'$ sont des entiers, donc $\mathcal{G}$ est au moins égal à n. On voit même que, pour avoir $\mathcal{G} = n$, il faut que l'on ait

$$\alpha = 1 \text{ ou } = n-1, \quad \mathcal{A} = 1, \quad \mathcal{G}' = 1,$$

et alors le système proposé G est évidemment composé des $1.2.3\ldots(n-1)$ substitutions de $n-1$ lettres.

La formule précédente montre encore que, si $\mathcal{G}$ est supérieur à n, cet indice est au moins égal à la plus petite des valeurs

$$2n, \quad \frac{n(n-1)}{2}.$$

Sur la limite des indices supérieurs à 2, dans le cas des systèmes transitifs.

460. Nous présenterons ici avec quelques modifications la démonstration que Cauchy a donnée du théorème de M. Bertrand, dans un Mémoire inséré au tome XXI des *Comptes rendus de l'Académie des Sciences*.

D'après ce qui précède, l'indice d'un système intransitif ne peut être inférieur au nombre des lettres; donc, pour établir le théorème que nous avons en vue, il suffit de considérer les systèmes transitifs.

Je dis que l'indice d'un système transitif G relatif

à n lettres ne peut être en même temps supérieur à 2 et inférieur à n, à moins que n ne soit égal à 4. Pour cela nous distinguerons trois cas.

1° *Le système* G *est simplement transitif.* — Dans ce cas le système G', qui comprend celles des substitutions de G qui ne déplacent que $n-1$ lettres, est intransitif et son indice est égal ou supérieur à $n-1$. Cet indice est aussi celui de G, et je dis qu'il ne peut pas être égal à $n-1$ si n est >4. En effet, si G et G' avaient $n-1$ pour indice, le système G' (n° 459) serait formé par les substitutions de $n-2$ lettres, et ces substitutions feraient partie de G; or le système G ne peut pas contenir toutes les substitutions de $n-1$ lettres, car autrement il ne serait pas transitif, ou il serait composé de toutes les substitutions des n lettres, et alors son indice serait égal à 1. Cela étant, si n est >4, on ne peut pas admettre que le système G, d'indice $n-1$, renferme toutes les substitutions de $n-2$ lettres; car, si cela avait lieu, l'indice de ce système serait égal à l'un des nombres $\frac{n(n-1)}{2}$, $n(n-1)$ (n° 441, *Corollaire*), ce qui implique contradiction. Donc, si n est >4, l'indice de G' ou de G est au moins égal (n° 459) au plus petit des deux nombres $2(n-1)$, $\frac{(n-1)(n-2)}{2}$. Par suite cet indice est supérieur à n.

2° *Le système* G *est deux fois transitif.* — Alors le système G' est simplement transitif, et si l'on a $n-1>4$, l'indice de ce système, qui est aussi celui de G, sera au moins égal au plus petit des deux nombres

$$2(n-2)=n+(n-4),$$
$$\frac{(n-2)(n-3)}{2}=n+\frac{(n-1)(n-6)}{2},$$

lesquels ne sont pas inférieurs à n, quand n est supérieur

à 5. Nous nous référons pour le cas de $n = 5$ au théorème du n° 415.

3° *Le système* G *est au moins trois fois transitif.* — Soient $a_0, a_1, \ldots, a_{n-1}$ les lettres données et

$$1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1}$$

les substitutions de G. Désignons aussi par T_i la transposition $(a_0 a_i)$. Si l'on multiplie la droite, pour fixer les idées, par

$$T_0,\ T_1,\ \ldots,\ T_{n-1}$$

les substitutions de G, on obtiendra $n\mu$ produits qui seront distincts, si l'indice de G est supérieur à 2; car si l'on avait

$$T_i S_k = T_j S_h,$$

on en conclurait

$$T_i^{-1} T_j = S_k S_h^{-1},$$

et par conséquent la substitution $T_i^{-1} T_j$ ferait partie de G. Or ce produit est une substitution circulaire de trois lettres, à moins que l'un de ses facteurs ne soit égal à 1, et dans ce cas elle se réduit à une transposition. D'ailleurs, dans notre hypothèse, le système G ne peut renfermer une telle substitution (n° 455, *Corollaire*); donc les $n\mu$ produits que nous avons formés sont distincts, ce qui exige que $n\mu$ ne soit pas supérieur à $1.2\ldots n$, c'est-à-dire que l'indice de G soit au moins égal à n.

CHAPITRE IV.

SUR QUELQUES CAS PARTICULIERS DE LA THÉORIE DES SUBSTITUTIONS.

Sur les fonctions linéaires de la forme $\frac{ax+b}{a'x+b'}$.

461. Les développements que je me propose de présenter ici nous conduiront à des conséquences intéressantes au point de vue de la théorie des substitutions, et ils trouveront en outre plus loin leur application dans la théorie des équations.

Soit posé

$$(1) \qquad \theta x = \frac{ax+b}{a'x+b'},$$

a, b, a', b' étant des quantités quelconques données; faisons aussi

$$\theta^2 x = \theta\theta x, \quad \theta^3 x = \theta\theta^2 x, \quad \ldots, \quad \theta^m x = \theta\theta^{m-1} x;$$

il est très-aisé d'avoir l'expression générale de $\theta^m x$. Soit en effet

$$(2) \qquad \theta^m x = \frac{a_m x + b_m}{a'_m x + b'_m},$$

on pourra écrire, d'après la loi de formation des fonctions $\theta^2 x$, $\theta^3 x$, ...,

$$(3) \qquad \begin{cases} a_m = a\, a_{m-1} + b\, a'_{m-1}, \\ a'_m = a'\, a_{m-1} + b'\, a'_{m-1}, \\ b_m = a\, b_{m-1} + b\, b'_{m-1}, \\ b'_m = a'\, b_{m-1} + b'\, b'_{m-1}. \end{cases}$$

Pour tirer de ces équations les valeurs de a_m, a'_m, b_m, b'_m, en fonction des quantités connues a, a', b, b', désignons

par z une quantité telle, que l'on ait

$$(4)\qquad \frac{z}{1} = \frac{b + b'z}{a + a'z},$$

les équations (3) donneront

$$a_m + a'_m z = (a + a'z)(a_{m-1} + a'_{m-1} z),$$
$$b_m + b'_m z = (a + a'z)(b_{m-1} + b'_{m-1} z);$$

d'où l'on tire

$$(5)\qquad \begin{cases} a_m + a'_m z = (a + a'z)^m, \\ b_m + b'_m z = z(a + a'z)^m. \end{cases}$$

En outre, l'équation (4), qui est du deuxième degré, a deux racines, et si l'on désigne ces racines par z et z', on aura encore

$$(6)\qquad \begin{cases} a_m + a'_m z' = (a + a'z')^m, \\ b_m + b'_m z' = z'(a + a'z')^m. \end{cases}$$

Les équations (5) et (6) déterminent les valeurs de a_m, a'_m, b_m, b'_m.

En faisant, pour abréger,

$$(7)\qquad 2t = \sqrt{(a + b')^2 - 4(ab' - ba')},$$

et

$$(8)\qquad \begin{cases} P_m = (a + b' + 2t)^m + (a + b' - 2t)^m, \\ Q_m = \dfrac{(a + b' + 2t)^m - (a + b' - 2t)^m}{2t}, \end{cases}$$

on trouve aisément

$$(9)\qquad \begin{cases} a_m = \dfrac{P_m + (a - b')Q_m}{2^{m+1}}, \\ a'_m = a' \dfrac{Q_m}{2^m}, \\ b_m = b \dfrac{Q_m}{2^m}, \\ b'_m = \dfrac{P_m - (a - b')Q_m}{2^{m+1}}, \end{cases}$$

équations dont on déduit

$$(10)\quad \left\{\begin{aligned} &\frac{a_m - b'_m}{a'_m} = \frac{a - b'}{a'},\\ &\frac{b_m}{a'_m} = \frac{b}{a'},\\ &a_m b'_m - b_m a'_m = (ab' - ba')^m; \end{aligned}\right.$$

en sorte que, si l'on a

$$ab' - ba' = \pm 1,$$

on aura aussi

$$a_m b'_m - b_m a'_m = \pm 1.$$

462. On connaît donc les coefficients de la fonction $\theta^m x$ en fonction des quantités connues a, b, a', b'. A la vérité, notre analyse semble en défaut si t est nulle, car, dans ce cas, les racines z et z' étant égales, les équations (6) ne diffèrent pas des équations (5); mais, comme les équations (8) et (9) ont lieu quelque petite que soit t, il en résulte qu'elles subsistent pour $t = 0$: on a, dans ce cas,

$$P_m = 2(a + b')^m,$$
$$Q_m = 2m(a + b')^{m-1};$$

et, par suite,

$$(11)\quad \left\{\begin{aligned} &a_m = \frac{(a + b')^m + m(a - b')(a + b')^{m-1}}{2^m},\\ &a'_m = \frac{ma'(a + b')^{m-1}}{2^{m-1}},\\ &b_m = \frac{mb(a + b')^{m-1}}{2^{m-1}},\\ &b'_m = \frac{(a + b')^m - m(a - b')(a + b')^{m-1}}{2^m}. \end{aligned}\right.$$

Ici les quantités a, b, a', b' doivent vérifier l'équation

$$(12)\qquad (a + b')^2 = 4(ab' - ba'),$$

et l'on peut écrire la valeur de $\theta^m x$ comme il suit :

$$\theta^m x = \frac{\left(a - b' + \frac{a + b'}{m}\right)x + 2b}{2a'x - \left(a - b' - \frac{a + b'}{m}\right)}.$$

On voit que, si l'on fait croître indéfiniment le nombre m, $\theta^m x$ converge vers la quantité

$$\frac{(a - b')x + 2b}{2a'x - (a - b')}$$

qui a pour valeur l'une des constantes $\frac{a - b'}{2a'}$, $\frac{-2b}{a - b'}$, lesquelles sont égales entre elles en vertu de la relation (12).

463. Proposons-nous maintenant de trouver la condition nécessaire et suffisante pour que l'on ait identiquement

$$(13) \qquad \theta^\mu x = x,$$

c'est-à-dire

$$(14) \qquad a_\mu = b'_\mu, \quad a'_\mu = 0, \quad b_\mu = 0.$$

On voit immédiatement qu'on doit exclure le cas particulier où l'on aurait

$$(a + b')^2 = 4(ab' - ba'),$$

car les équations (11) montrent que, pour satisfaire aux équations (14), il faudrait que l'on eût

$$a + b' = 0,$$

par suite,

$$ab' - ba' = 0,$$

et alors la fonction θx ne dépendrait pas de x. Cela étant, on voit par les équations (9) que, pour satisfaire aux équations (14), il est nécessaire et suffisant que l'on ait

$$Q_\mu = 0,$$

ou

$$(a + b' + 2t)^\mu - (a + b' - 2t)^\mu = 0.$$

On tire de là

$$a + b' + 2t = (a + b' - 2t)\left(\cos\frac{2\lambda\pi}{\mu} + \sqrt{-1}\sin\frac{2\lambda\pi}{\mu}\right)$$

et

$$(15) \qquad 2t = (a + b')\tang\frac{\lambda\pi}{\mu}\sqrt{-1},$$

en désignant par λ un nombre entier qu'on doit supposer premier avec μ pour qu'il faille effectivement exécuter μ fois sur x l'opération désignée par θ avant de reproduire x.

La comparaison de cette valeur de $2t$ avec celle qu'on tire de l'équation (7) donne

$$(16) \qquad (a + b')^2 - 4(ab' - ba')\cos^2\frac{\lambda\pi}{\mu} = 0;$$

ce qui est la condition nécessaire et suffisante pour que l'on ait

$$\theta^\mu x = x.$$

Si l'on suppose que les quantités a, b, a', b' soient réelles, l'équation (16) montre que la quantité $ab' - ba'$ doit être positive, le cas de $\mu = 2$ étant excepté. Et comme on peut, sans changer la fonction θx, multiplier les constantes a, b, a', b' par un facteur quelconque, on voit que, sans altérer la généralité de la solution, on peut supposer

$$(17) \qquad ab' - ba' = 1;$$

alors l'équation (16) donne

$$(18) \qquad a + b' = 2\cos\frac{\lambda\pi}{\mu}.$$

Nous ne mettons pas le signe $\pm$ devant le second membre, parce qu'on peut, si on le juge à propos, changer les signes des quatre quantités a, b, a', b'.

Des équations (17) et (18) on tire

$$(19)\qquad \left\{\begin{aligned} b' &= -\left(a - 2\cos\frac{\lambda\pi}{\mu}\right),\\ b &= -\frac{a^2 - 2a\cos\frac{\lambda\pi}{\mu} + 1}{a'}; \end{aligned}\right.$$

et la fonction θx a pour valeur

$$(20)\qquad \theta x = \frac{ax - \dfrac{a^2 - 2a\cos\frac{\lambda\pi}{\mu} + 1}{a'}}{a'x - \left(a - 2\cos\frac{\lambda\pi}{\mu}\right)}.$$

Les quantités a et a' demeurent indéterminées; quant à λ, c'est un nombre entier quelconque premier avec μ. Si l'on continue de poser

$$\theta^m x = \frac{a_m x + b_m}{a'_m x + b'_m},$$

on trouvera aisément

$$(21)\qquad \left\{\begin{aligned} a_m &= \frac{a\sin\frac{m\lambda\pi}{\mu} - \sin\frac{(m-1)\lambda\pi}{\mu}}{\sin\frac{\lambda\pi}{\mu}},\\ a'_m &= a'\,\frac{\sin\frac{m\lambda\pi}{\mu}}{\sin\frac{\lambda\pi}{\mu}},\\ b_m &= -\frac{a^2 - 2a\cos\frac{\lambda\pi}{\mu} + 1}{a'}\;\frac{\sin\frac{m\lambda\pi}{\mu}}{\sin\frac{\lambda\pi}{\mu}},\\ b'_m &= \frac{\sin\frac{(m+1)\lambda\pi}{\mu} - a\sin\frac{m\lambda\pi}{\mu}}{\sin\frac{\lambda\pi}{\mu}}. \end{aligned}\right.$$

Des équations (19) et (21) on tire

$$(22)\qquad \left\{\begin{aligned} b'_m &= -\left(a_m - 2\cos\frac{m\lambda\pi}{\mu}\right),\\ b_m &= -\frac{a_m^2 - 2a_m\cos\frac{m\lambda\pi}{\mu} + 1}{a'_m}\end{aligned}\right.$$

et

$$(23)\qquad \left\{\begin{aligned} a &= \frac{a_m\sin\frac{\lambda\pi}{\mu} + \sin\frac{(m-1)\lambda\pi}{\mu}}{\sin\frac{m\lambda\pi}{\mu}};\\ a' &= a'_m\,\frac{\sin\frac{\lambda\pi}{\mu}}{\sin\frac{m\lambda\pi}{\mu}},\\ b &= -\frac{a_m^2 - 2a_m\cos\frac{m\lambda\pi}{\mu} + 1}{a'_m}\,\frac{\sin\frac{\lambda\pi}{\mu}}{\sin\frac{m\lambda\pi}{\mu}},\\ b' &= \frac{\sin\frac{(m+1)\lambda\pi}{\mu} - a_m\sin\frac{\lambda\pi}{\mu}}{\sin\frac{m\lambda\pi}{\mu}}.\end{aligned}\right.$$

Ces formules permettent de résoudre la question suivante :

Étant donnée une fonction linéaire $\frac{a_m x + b_m}{a'_m x + b'_m}$, *trouver une fonction linéaire* $\theta x = \frac{ax + b}{a'x + b'}$ *telle, que l'on ait identiquement*

$$\theta^m x = \frac{a_m x + b_m}{a'_m x + b'_m} \quad \text{et} \quad \theta^\mu x = x.$$

On voit que le problème n'est possible que si les quantités données a_m, b_m, a'_m, b'_m satisfont aux équations (22).

Des fonctions rationnelles linéaires prises suivant un module premier.

464. Nous allons considérer ici, à un point de vue particulier, les fonctions rationnelles linéaires de la forme

$$(1) \qquad \theta z = \frac{az + b}{a'z + b'},$$

dans laquelle z est une variable indépendante. Nous supposerons que les constantes a, b, a', b' soient des nombres entiers positifs, nuls ou négatifs, et nous conviendrons, en outre, de prendre les résultats suivant un module premier impair p; en d'autres termes, nous regarderons comme équivalents les entiers qui sont congrus relativement au module. Les développements qui vont suivre conduisent à des conséquences intéressantes pour la théorie des nombres et qui sont surtout utiles dans la théorie des substitutions; je les ai présentés, pour la première fois, dans un article inséré au tome XLVIII des *Comptes rendus de l'Académie des Sciences*.

Comme nous faisons abstraction du cas où θz se réduit à une constante, la différence $ab' - ba'$ ne sera jamais congrue à zéro suivant le module p; cette différence sera dite le *déterminant* de la fonction linéaire θz. On peut, sans changer cette fonction, multiplier les quatre constantes a, b, a', b' par un même nombre k; le déterminant se trouve alors multiplié par k^2, et il sera, après comme avant la multiplication, résidu quadratique ou non-résidu quadratique de p. D'après cela, nos fonctions linéaires peuvent être classées en deux genres; le premier genre comprendra les fonctions dont le déterminant est résidu quadratique, tandis que celles dont le déterminant est non-résidu constitueront le deuxième

genre. Mais on voit que l'on pourra toujours faire en sorte que, dans le premier genre, le déterminant soit un résidu quadratique quelconque donné, 1 par exemple, et pareillement que, dans le deuxième genre, le déterminant soit un non-résidu quelconque donné.

L'expression générale de θz comprend des fonctions entières et des fonctions fractionnaires; les premières peuvent être ramenées à la forme

$$f + \Delta z, \tag{2}$$

et les dernières à la forme

$$f - \frac{\Delta}{z + g}, \tag{3}$$

Δ désignant dans les deux cas le déterminant de la fonction.

Dans les formules (2) et (3), le déterminant Δ peut recevoir les $p - 1$ valeurs

$$1, 2, \ldots, p - 1,$$

parmi lesquelles il y a autant de résidus que de non-résidus; les constantes f et g peuvent recevoir les mêmes valeurs, et, en outre, la valeur zéro. Il s'ensuit que le nombre des fonctions entières est $p(p-1)$ en comprenant la variable z elle-même, et que celui des fonctions fractionnaires est $p^2(p-1)$; par conséquent, le nombre total N des fonctions linéaires suivant le module p est

$$N = (p+1)p(p-1), \tag{4}$$

et le nombre des fonctions du premier ou du deuxième genre est $\frac{1}{2}$N.

465. Soient θz et $\theta_1 z$ deux fonctions rationnelles linéaires prises suivant le module p; pour abréger le discours, nous nommerons *produit de la fonction linéaire*

$\theta_1 z$ par θz le résultat $\theta\theta_1 z$ que l'on obtient en exécutant d'abord sur la variable z l'opération désignée par θ_1, puis sur le résultat $\theta_1 z$ l'opération désignée par θ; cette définition s'étend naturellement au cas de trois, de quatre, etc., fonctions linéaires. Le produit de m fonctions linéaires égales à θz, c'est-à-dire le résultat que l'on obtient en exécutant m fois sur z l'opération θ, sera la $m^{\text{ième}}$ puissance de θz, et nous la représenterons par $\theta^m z$.

Le produit de deux fonctions linéaires a pour déterminant le produit des déterminants des facteurs. Si, en effet, on pose

$$\theta z = \frac{az+b}{a'z+b'}, \quad \theta_1 z = \frac{a_1 z + b_1}{a'_1 z + b'_1},$$

on aura

$$\theta\theta_1 z = \frac{(aa_1 + ba'_1)z + (ab_1 + bb'_1)}{(a'a_1 + b'a'_1)z + (a'b_1 + b'b'_1)} = \frac{Az+B}{A'z+B'},$$

et

$$(AB' - BA') = (ab' - ba')(a_1 b'_1 - b_1 a'_1).$$

On conclut de là que le produit de tant de fonctions linéaires que l'on voudra est une fonction linéaire dont le déterminant est égal au produit des déterminants des facteurs; d'où il suit que la fonction produit appartiendra au premier ou au deuxième genre, suivant que le nombre des facteurs du deuxième genre sera pair ou impair.

Il est évident que l'ensemble de toutes les fonctions linéaires forme un groupe tel, que le produit de plusieurs fonctions du groupe fait aussi partie de ce groupe. On voit par ce qui précède qu'il en est de même de l'ensemble des seules fonctions linéaires du premier genre, mais non pas de l'ensemble des seules fonctions du deuxième genre.

466. Considérons la série indéfinie

$$(5) \qquad z,\ \theta z,\ \theta^2 z,\ \theta^3 z,\ \ldots,$$

formée par la variable z et les diverses puissances de la fonction linéaire θz pour le module premier p. Comme le nombre des fonctions linéaires est limité, la suite précédente ne pourra jamais offrir qu'un nombre fini de valeurs distinctes suivant le module p, et, par conséquent, quelques-uns des termes de cette série se trouveront nécessairement reproduits une infinité de fois. Supposons que l'on ait identiquement

$$\theta^{n+m} z \equiv \theta^m z \quad \text{ou} \quad \theta^n \theta^m z \equiv \theta^m z \pmod{p},$$

on pourra écrire z au lieu de $\theta^m z$, et l'on aura identiquement

$$(6) \qquad \theta^n z \equiv z \pmod{p},$$

d'où l'on conclut aisément

$$\theta^{\lambda n+\rho} z \equiv \theta^\rho z \pmod{p},$$

quels que soient les entiers positifs λ et ρ. On peut convenir d'étendre cette formule à toutes les valeurs positives, nulles ou négatives de ρ, en sorte que l'on aura en particulier

$$(7) \qquad \theta^0 z \equiv z \pmod{p}$$

et

$$(8) \qquad \theta^{-1} z \equiv \theta^{n-1} z \pmod{p}.$$

Si n désigne le plus petit nombre tel, que la congruence (6) ait lieu identiquement, la série (5) ne comprendra que les n termes distincts

$$(9) \qquad z,\ \theta z,\ \theta^2 z,\ \ldots,\ \theta^{n-1} z,$$

et deux quelconques de ces termes seront effectivement incongrus suivant le module p, au moins tant que z

restera indéterminé ; le nombre n sera dit l'*ordre* de la fonction linéaire θz pour le module p.

Si e est un nombre premier avec n et inférieur à n, la fonction $\theta^e z$ sera, comme θz, de l'ordre n ; car, si l'on suppose les termes de la suite (9) rangés en cercle et qu'on les compte de e en e à partir du premier z, c'est-à-dire en suivant l'ordre

$$z,\ \theta\ z,\ \theta^{2e} z,\ \ldots,$$

il est clair qu'on ne reviendra au point de départ qu'après avoir rencontré les n termes. Au contraire, si les nombres n et e ont un plus grand commun diviseur d supérieur à 1, on se trouvera ramené au point de départ après avoir rencontré $\frac{n}{d}$ termes, et l'ordre de la fonction $\theta^e z$ sera égal à $\frac{n}{d}$.

La fonction $\theta^{-1} z$, définie par la congruence (8), sera dite l'*inverse* de θz ; on peut obtenir immédiatement sa valeur ; car, si l'on remplace z par $\theta^{-1} z$ dans la congruence (1), il vient

$$\theta\theta^{-1} z \equiv z \equiv \frac{a\theta^{-1} z + b}{a'\theta^{-1} z + b'},$$

d'où

$$(10) \qquad \theta^{-1} z \equiv \frac{-b'z + b}{a'z - a},$$

en sorte que les fonctions θz et $\theta^{-1} z$ se déduisent l'une de l'autre en changeant a et b' en $-b'$ et $-a$.

467. Soit, comme précédemment,

$$\theta z \equiv \frac{az + b}{a'z + b'},$$

et posons en outre

$$(11) \qquad \theta^m z \equiv \frac{a_m z + b_m}{a'_m z + b'_m};$$

si l'on fait, pour abréger, comme au n° **461**,

$$(12) \qquad 2t = \sqrt{(a+b')^2 - 4(ab' - ba')},$$

$$(13) \qquad \begin{cases} P_m = (a+b'+2t)^m + (a+b'-2t)^m, \\ Q_m = \dfrac{(a+b'+2t)^m - (a+b'-2t)^m}{2t}, \end{cases}$$

on aura les équations déjà considérées

$$(14) \qquad \begin{cases} a_m = \dfrac{P_m + (a-b')Q_m}{2^{m+1}}, \quad b_m = b\dfrac{Q_m}{2^m}, \\ a'_m = a'\dfrac{Q_m}{2^m}, \quad b'_m = \dfrac{P_m - (a-b')Q_m}{2^{m+1}}, \end{cases}$$

et qui sont comprises dans les formules

$$(15) \qquad a_m + b'_m = \frac{P_m}{2^m}, \quad \frac{a_m - b'_m}{a - b'} = \frac{b_m}{b} = \frac{a'_m}{a'} = \frac{Q_m}{2^m}.$$

Désignons par Δ le déterminant $ab' - ba'$ de la fonction θz et par Δ_m celui de $\theta^m z$; posons en outre

$$(16) \qquad 2t_m = \sqrt{(a_m + b'_m)^2 - 4(a_m b'_m - b_m a'_m)};$$

on aura, par les formules (14) ou (15),

$$(17) \qquad \frac{t_m}{t} = \frac{Q_m}{2^m}, \quad \Delta_m = \Delta^m.$$

On voit que, dans le passage de la fonction θz à sa $m^{\text{ième}}$ puissance $\theta^m z$, les rapports des quantités $a - b'$, b, a', t à l'une d'elles restent invariables et que le déterminant se trouve remplacé par sa $m^{\text{ième}}$ puissance; cette dernière propriété résulte d'ailleurs de ce qui a été dit plus haut.

Les formules (14) montrent que $\theta^m z$ ne peut jamais être une fonction entière autre que z, à moins que θz ne soit elle-même entière; car, si a' n'est pas nul, a'_m ne peut s'évanouir que dans le cas où l'on a $Q_m = 0$, et alors on a $b_m = 0$ et $a_m = b'_m$.

Pour satisfaire à la congruence (6), il faut et il suffit que l'on ait

$$(18) \qquad Q_n \equiv 0 \pmod{p};$$

mais, pour que n soit effectivement l'ordre de la fonction θz, il faut en outre que pour toute valeur de m inférieure à n la quantité Q_m soit différente de zéro ; nous faisons ici abstraction du cas où θz est du premier ordre, c'est-à-dire du cas où θz se réduit à z.

Nous nous proposons d'étudier les fonctions linéaires θz au point de vue de leur ordre. Il convient dans cette recherche de distinguer trois cas, suivant que la quantité t^2 est congrue à zéro suivant le module p, résidu quadratique de ce module, ou non-résidu quadratique.

468. Examinons d'abord le premier cas où la quantité t^2 est congrue à zéro suivant le module p; la congruence (18) devient alors

$$2n(a+b')^{n-1} \equiv 0 \pmod{p}.$$

On ne peut pas avoir $a+b' \equiv 0 \pmod{p}$, car autrement la condition $t \equiv 0 \pmod{p}$ se réduirait à

$$ab' - ba' \equiv 0 \pmod{p};$$

le déterminant de θz serait nul et cette fonction se réduirait à une constante. La congruence (18) ne peut donc avoir lieu que si n est un multiple de p, et par conséquent, dans le cas qui nous occupe, l'ordre de la fonction linéaire θz est toujours égal au module p. La condition $t \equiv 0 \pmod{p}$ donne

$$a + b' \equiv 2\sqrt{\Delta} \pmod{p};$$

d'où il suit que le déterminant Δ est résidu quadratique de p, et, par conséquent, la fonction θz appartient au premier genre.

On obtiendra toutes les fonctions linéaires d'ordre p en prenant tous les systèmes de solutions distinctes des deux congruences

$$a + b' \equiv 2\sqrt{\Delta}, \quad ab' - ba' \equiv \Delta \quad (\text{mod. } p);$$

si l'on veut d'abord les fonctions entières, on posera $a' = 0$, $b' = 1$, ce qui donnera $a = \Delta = 1$; on aura donc les $p - 1$ fonctions d'ordre p

$$(19) \qquad \theta z = z + b,$$

en prenant pour b les valeurs successives $1, 2, \ldots, p-1$. Pour avoir les fonctions fractionnaires, nous ferons $a' = 1$ et nous poserons

$$a - b' \equiv 2g,$$

ce qui donnera

$$a \equiv \sqrt{\Delta} + g, \quad b' \equiv \sqrt{\Delta} - g, \quad b \equiv -g^2,$$

en sorte que l'expression des fonctions fractionnaires d'ordre p sera

$$(20) \qquad \theta z = \frac{(\sqrt{\Delta} + g)z - g^2}{z + \sqrt{\Delta} - g} = g + \sqrt{\Delta} - \frac{\Delta}{z + \sqrt{\Delta} - g}.$$

On peut attribuer à la quantité g les p valeurs

$$0, \; 1, \; 2, \; \ldots, \; p - 1,$$

et à la quantité $\sqrt{\Delta}$ les mêmes valeurs, zéro excepté. on obtiendra ainsi $p(p-1)$ fonctions fractionnaires. Il suit de là que le nombre total N_p des fonctions linéaires d'ordre p est

$$(21) \qquad N_p = (p+1)(p-1).$$

Comme tout nombre inférieur à p est premier avec ce nombre, toutes les puissances d'une fonction linéaire d'ordre p sont aussi de cet ordre; il en résulte que les

N_p fonctions dont nous venons d'établir l'existence forment $p+1$ groupes renfermant chacun $p-1$ fonctions qui sont les puissances de l'une quelconque d'entre elles. Les $p-1$ fonctions comprises dans la formule (19) constituent évidemment l'un de ces groupes, et l'on obtiendra les p autres groupes par la formule (20) en associant successivement chacune des p valeurs de g avec le système des $p-1$ valeurs de $\sqrt{\Delta}$. Effectivement, si l'on forme, en se servant des formules (14) ou (15), la puissance $m^{\text{ième}}$ de la fonction θz donnée par l'équation (20), on trouve

$$(22) \qquad \theta^m z = \frac{\left(\frac{1}{m}\sqrt{\Delta} + g\right)z - g^2}{z - \left(\frac{1}{m}\sqrt{\Delta} - g\right)},$$

expression qui se déduit de celle de θz par le seul changement de $\sqrt{\Delta}$ en $\frac{1}{m}\sqrt{\Delta}$.

469. Lorsque la quantité t^2 est différente de zéro, la congruence (18), savoir

$$(23) \qquad (a + b' + 2t)^n \equiv (a + b' - 2t)^n \pmod{p},$$

peut être mise sous la forme

$$(24) \qquad a + b' + 2t \equiv i(a + b' - 2t) \pmod{p},$$

en désignant par i une racine de la congruence

$$(25) \qquad i^n \equiv 1 \pmod{p}.$$

En outre, pour que n soit effectivement l'ordre de la fonction θz, il est nécessaire que i soit une racine primitive de la congruence précédente.

Si, dans la congruence (24), on substitue à t sa valeur tirée de la formule (12), puis qu'on fasse disparaître, par

l'élévation au carré, le radical introduit, il viendra

$$(26)\qquad \frac{(a - b')^2}{ab' - ba'} \equiv \frac{(i + 1)^2}{i} \quad (\text{mod. } p);$$

telle est la condition à laquelle doivent satisfaire les constantes a, b, a', b', pour que le nombre n soit l'ordre de la fonction θz, dans l'hypothèse où t est différent de zéro. Si l'on pose

$$(27)\qquad a - b' = 2g,$$

on pourra, au moyen des formules (12), (24) et (27), exprimer les quantités a, b', ba' et le déterminant Δ en fonction des quantités g, t, i; on trouve ainsi

$$(28)\qquad \left\{\begin{aligned} a &= \frac{i+1}{i-1}\,t + g,\\ b' &= \frac{i+1}{i-1}\,t - g,\\ ba' &= t^2 - g^2,\\ \Delta &= -\frac{4it^2}{(i-1)^2}. \end{aligned}\right.$$

Ces formules serviront à construire les fonctions linéaires que nous considérons; on pourra faire $a' = 1$ quand cette quantité a' ne sera pas nulle. Il est aisé de former aussi la puissance $m^{\text{ième}}$ de θz, savoir

$$\theta^m z = \frac{a_m z + b_m}{a'_m z + b'_m};$$

on trouve, en faisant usage des formules (14) ou (15) et en supprimant un facteur commun, ce qu'il est permis de faire,

$$(29)\qquad a_m + b'_m = 2t\,\frac{i^m + 1}{i^m - 1},\quad a_m - b'_m = a - b',\quad a'_m = a',\quad b_m = b.$$

en sorte qu'on passe de l'expression de θz à celle de $\theta^m z$ en remplaçant simplement i par i^m sans changer les valeurs de g et de t.

470. Supposons que la quantité

$$t^2 = \left(\frac{a+b'}{2}\right)^2 - (ab' - ba')$$

soit résidu quadratique du module p. Alors les quantités t et i, respectivement définies par les formules (12) et (24), sont l'une et l'autre réelles ; par suite, i ne peut être racine primitive de la congruence (25) que dans le cas où l'ordre n de la fonction θz est égal à $p-1$ ou à un diviseur de $p-1$. Les fonctions linéaires qui répondent à une racine primitive i de la congruence (25) peuvent être formées immédiatement au moyen des formules (28).

Pour avoir en premier lieu les fonctions entières, on fera $a'=0$, $b'=1$, et l'on aura ces deux solutions :

$$t = g = \frac{i-1}{2}, \quad a = i \quad \text{et} \quad t = -g = \frac{i-1}{2i}, \quad a = \frac{1}{i},$$

qui donneront les $2p$ fonctions entières $iz+b$, $\frac{1}{i}z+b$ si l'on attribue à b les valeurs successives $0, 1, 2, \ldots, p-1$. Mais nous considérerons seulement les p fonctions fournies par la première formule

$$(30) \qquad iz + b$$

comme appartenant à la racine i ; les p autres seront relatives à la racine primitive $\frac{1}{i}$ si n est > 2, et, dans le cas particulier de $n=2$, elles coïncideront avec celles de la formule (30).

Pour avoir en second lieu les fonctions fractionnaires,

on fera $a' = 1$ dans les formules (28) et l'on aura

$$(31)\quad \begin{cases} a = \dfrac{i+1}{i-1}\,t + g, & b = t^2 - g^2, \quad a' = 1, \\[2ex] b' = \dfrac{i+1}{i-1}\,t - g, & \Delta = \dfrac{4it^2}{(i-1)^2}; \end{cases}$$

le changement de t en $-t$ dans les formules (31) équivaut au changement de i en $\frac{1}{i}$; donc, lorsqu'on doit employer successivement toutes les racines i, on peut se borner à donner à t toutes les $\frac{p-1}{2}$ valeurs

$$1,\ 2,\ \ldots,\ \frac{p-1}{2}.$$

Quant à la quantité g, elle peut recevoir les p valeurs

$$0,\ 1,\ 2,\ \ldots,\ p-1.$$

On obtiendra de la sorte, au moyen des formules (31), $\frac{p(p-1)}{2}$ fonctions fractionnaires relatives à la racine i, ce qui, avec les p fonctions entières, donnera un total de $\frac{1}{2}(p+1)p$ fonctions linéaires. Et cela aura lieu encore dans le cas de $n = 2$, bien qu'alors la congruence (25) n'ait que la seule racine primitive -1, car, cette racine étant égale à son inverse, les formules (31) ne changeront pas par le changement de t en $-t$.

Il est facile de voir que les $\frac{1}{2}(p+1)p$ fonctions qui répondent à une racine i sont distinctes de celles qui se rapportent à une deuxième racine primitive, en sorte que, si $\varphi(n)$ désigne le nombre des racines primitives de la congruence (25), il y aura un nombre de fonctions

d'ordre n égal à

$$\frac{1}{2}(p+1)p\varphi(n),$$

pour lesquelles la quantité t^2 est résidu quadratique de p. En particulier, le nombre des fonctions linéaires d'ordre $p-1$ sera

$$\frac{1}{2}(p+1)p\varphi(p-1),$$

$\varphi(p-1)$ désignant ici le nombre des racines primitives pour le nombre premier p.

Quant au nombre total des fonctions linéaires pour lesquelles t^2 est résidu quadratique de p, et dont l'ordre n est en conséquence un diviseur de $p-1$, il sera donné par la formule

$$N_{p-1} = \frac{1}{2}(p+1)p\sum\varphi(n);$$

l'expression $\sum\varphi(n)$, qui s'étend à tous les diviseurs n de $p-1$, 1 excepté, est égale, comme on sait, à $p-2$; on aura donc

$$(32)\qquad N_{p-1} = \frac{1}{2}(p+1)p(p-2).$$

Ces N_{p-1} fonctions linéaires peuvent être partagées en $\frac{1}{2}(p+1)p$ groupes contenant chacun $p-2$ fonctions, qui sont les $p-2$ puissances d'une fonction linéaire d'ordre $p-1$ relative à une racine primitive donnée de p.

En effet, il est évident que toutes les N_{p-1} fonctions que nous considérons seront données par les formules (30) et (31), en employant toutes les racines de la congruence

$$i^{p-1}-1\equiv 0 \pmod{p},$$

excepté 1; et ces racines ne sont autre chose que les

$p-2$ premières puissances d'une racine primitive i. Or, en employant cette racine primitive, les équations (30) et (31) donnent $\frac{1}{2}(p+1)p$ fonctions d'ordre $p-1$: d'ailleurs les formules (29) montrent que les puissances de ces fonctions se déduisent des fonctions elles-mêmes, en remplaçant la racine primitive i par ses puissances; on aura donc toutes les fonctions linéaires que nous considérons en prenant les $\frac{1}{2}(p+1)p$ qui répondent à la racine primitive donnée i, et en formant le groupe des $p-2$ premières puissances de chacune d'elles.

Les formules (31) montrent que Δ et i sont en même temps résidus ou non-résidus quadratiques de p ; il s'ensuit que les fonctions dont nous nous occupons appartiendront au premier ou au deuxième genre, suivant que la racine i à laquelle elles se rapportent sera résidu ou non-résidu quadratique de p. Or, pour les fonctions d'ordre $p-1$, i est non-résidu ; donc ces fonctions et leurs puissances impaires appartiennent au deuxième genre, tandis que les puissances paires appartiennent au premier genre. On voit aussi que, parmi nos N_{p-1} fonctions, il y en a

$$\frac{1}{4}(p+1)p(p-3)$$

qui appartiennent au premier genre, et

$$\frac{1}{4}(p+1)p(p-1)$$

qui appartiennent au deuxième genre.

471. Examinons maintenant le cas où la quantité

$$t^2=\left(\frac{a+b'}{2}\right)^2-(ab'-ba')$$

non-résidu quadratique du module p. Alors la quan- t est imaginaire, et pour que a et b' soient réelles, il t, par les formules (28), que la racine i soit elle-même iginaire, ou qu'elle soit égale à -1; dans ce dernier on a nécessairement $n = 2$. Je dis que généralement iombre n, qui marque l'ordre de la fonction θz, est l à $p+1$ ou à un diviseur de $p+1$. Si l'on a $n = 2$, roposition est évidente, car 2 divise $p+1$; supposons ic $n > 2$. Si l'on pose

$$) \qquad \frac{(a+b')^2}{ab'-ba'} = 2(k+1),$$

ongruence (26) devient

$$) \qquad i^2 - 2ki + 1 \equiv 0 \pmod{p}.$$

sait (n° 372, théorème III) que les racines de la con- ence irréductible (34) peuvent être représentées par i ^{p}, et, comme le produit de ces racines est congru à 1, a

$$) \qquad i^{p+1} \equiv 1 \pmod{p};$$

peut donc être racine primitive de la congruence (25) si n est égal à $p+1$ ou à un diviseur de $p+1$.
)'après la congruence (34), k désigne la demi-somme deux racines conjuguées i et $\frac{1}{i}$, et il en résulte que n a

$$\frac{i+1}{i-1}\,t = \sqrt{\frac{k+1}{k-1}\,t^2};$$

ıs attribuerons au radical qui figure dans le second mbre de cette formule celle de ses deux valeurs qui partie de la suite

$$1,\ 2,\ \ldots,\ \frac{p-1}{2};$$

la seconde valeur du radical sera alors relative à la racine $\frac{1}{i}$ inverse de i. Cela posé, comme l'hypothèse $a' = 0$ rendrait t^2 résidu quadratique de p, le cas que nous examinons ne comprend pas de fonctions entières ; on peut donc faire $a' = 1$ et les formules (28) donneront alors

$$(36)\quad \begin{cases} a = \sqrt{\dfrac{k+1}{k-1}\,t^2} + g, \quad b = t^2 - g^2, \quad a' = 1, \\ b' = \sqrt{\dfrac{k+1}{k-1}\,t^2} - g, \quad \Delta = \dfrac{2t^2}{k-1}. \end{cases}$$

Ces formules feront connaître les fonctions linéaires qui répondent à la racine i en donnant à g les p valeurs

$$0,\ 1,\ 2,\ \ldots,\ p-1,$$

et en prenant successivement pour t^2 tous les $\frac{p-1}{2}$ non-résidus. On aura ainsi $\frac{1}{2}p(p-1)$ fonctions linéaires d'ordre n relatives à la racine i, et il faut remarquer que l'on obtiendrait en même temps les puissances de ces fonctions en remplaçant la racine i par ses diverses puissances. On voit aussi que le nombre de toutes les fonctions d'ordre n que nous considérons est

$$\frac{1}{2}p(p-1)\varphi(n),$$

$\varphi(n)$ désignant, comme précédemment, le nombre des racines primitives de la congruence (25). Cette conclusion s'applique au cas de $n = 2$; alors on n'a que la seule racine primitive $i = -1$ qui donne aussi $k = -1$. Les formules (36) font ainsi connaître $\frac{1}{2}p(p-1)$ ou $\frac{1}{2}p(p-1)\varphi(2)$ fonctions linéaires du deuxième ordre

pour lesquelles t^2 est non-résidu quadratique de p. Si l'on suppose $n = p + 1$, on obtient l'expression

$$\frac{1}{2} p(p-1)\varphi(p+1)$$

du nombre des fonctions linéaires d'ordre $p+1$.

Enfin, si N_{p+1} désigne le nombre total des fonctions linéaires pour lesquelles t^2 est non-résidu quadratique de p, et dont l'ordre est en conséquence un diviseur de $p+1$, on aura

$$N_{p+1} = \frac{1}{2} p(p-1)\sum\varphi(n);$$

or l'expression $\sum\varphi(n)$, qui s'étend à tous les diviseurs des $p+1$ autres que 1, est égal à p; donc

$$(37) \qquad N_{p+1} = \frac{1}{2} p^2(p-1).$$

Ces N_{p+1} fonctions linéaires peuvent être partagées en $\frac{1}{2}p(p-1)$ groupes contenant chacun p fonctions, qui sont les p premières puissances d'une fonction linéaire d'ordre $p+1$, relative à une racine primitive donnée de p.

En effet, les N_{p+1} fonctions dont il s'agit seront données par les formules (36) en employant toutes les racines de la congruence (35), excepté 1, et ces racines ne sont autre chose que les p premières puissances d'une racine primitive i. Or, en employant cette racine primitive, les formules (36) donneront $\frac{1}{2} p(p-1)$ fonctions linéaires d'ordre $p+1$; d'ailleurs les puissances de ces fonctions se déduisent des fonctions elles-mêmes en remplaçant la racine primitive i par ses puissances; on aura donc toutes

les fonctions linéaires dont nous nous occupons en prenant parmi ces fonctions les $\frac{1}{2}p(p-1)$ qui répondent à la racine i, et en formant le groupe des p premières puissances de chacune d'elles.

Les formules (36) montrent que les quantités Δ et $\frac{k+1}{2}$ sont toutes deux résidus quadratiques de p, ou toutes deux non-résidus; je dis que ces quantités sont résidus ou non-résidus, suivant que l'ordre n de la fonction θz divise ou ne divise pas $\frac{p+1}{2}$. On a en effet, par la congruence (34),

$$\frac{k+1}{2} \equiv \frac{(i+1)^2}{4i} \pmod{p},$$

et, en élevant à la puissance $\frac{p-1}{2}$,

$$\left.\begin{aligned} \left(\frac{k+1}{2}\right)^{\frac{p-1}{2}} &\equiv \frac{(i+1)^{p-1}}{i^{\frac{p-1}{2}}} \equiv \frac{i(i+1)^p}{i^{\frac{p+1}{2}}(i+1)} \\ &\equiv \frac{i^{p+1}+i}{i^{\frac{p+1}{2}}(i+1)} \equiv \frac{1}{i^{\frac{p+1}{2}}} \end{aligned}\right\} \pmod{p};$$

mais on a

$$i^{\frac{p+1}{2}} \equiv +1 \quad \text{ou} \quad i^{\frac{p+1}{2}} \equiv -1 \pmod{p},$$

suivant que n divise ou ne divise pas $\frac{p+1}{2}$; on aura donc, dans les mêmes hypothèses,

$$\left(\frac{k+1}{2}\right)^{\frac{p-1}{2}} \equiv +1 \quad \text{ou} \quad \left(\frac{k+1}{2}\right)^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

c'est-à-dire

$$\Delta^{\frac{p-1}{2}} \equiv +1 \quad \text{ou} \quad \Delta^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Il résulte de là que les fonctions linéaires d'ordre $p+1$ appartiennent au deuxième genre, ainsi que leurs puissances impaires ; au contraire, les puissances paires appartiennent au premier genre. Donc, parmi nos fonctions dont le nombre est N_{p+1}, il y en a

$$\frac{1}{4}p(p-1)^2$$

qui appartiennent au premier genre, et

$$\frac{1}{4}(p+1)p(p-1)$$

qui sont du deuxième genre.

472. Si l'on ajoute l'unité et les trois nombres N_p, N_{p-1}, N_{p+1}, on doit retrouver le nombre N de toutes les fonctions linéaires prises suivant le module p ; on vérifie effectivement, au moyen des formules (4), (21), (32) et (37), que l'on a bien

$$N = 1 + N_p + N_{p-1} + N_{p+1};$$

si l'on désigne en outre par G le nombre des groupes distincts qui sont formés par les puissances d'une fonction linéaire d'ordre p, $p-1$ ou $p+1$, il est aisé de s'assurer que l'on a

$$G = p^2 + p + 1.$$

Il convient de remarquer les fonctions du deuxième ordre qui se distribuent dans les deux genres que nous avons distingués. Les unes sont les puissances de degré $\frac{p-1}{2}$ des fonctions d'ordre $p-1$, leur nombre est

$\frac{1}{2}p(p+1)$, et elles appartiennent au premier genre ou au deuxième genre suivant que $\frac{p-1}{2}$ est pair ou impair, c'est-à-dire suivant que p a la forme $4q+1$ ou la forme $4q+3$. Les autres sont les puissances du degré $\frac{p+1}{2}$ des fonctions d'ordre $p+1$; leur nombre est $\frac{1}{2}p(p-1)$, et elles appartiennent au premier ou au deuxième genre suivant que $\frac{p+1}{2}$ est pair ou impair, c'est-à-dire suivant que p a la forme $4q+3$ ou la forme $4q+1$. On voit que le nombre total des fonctions du deuxième ordre est égal à p^2. Dans ce cas de $n=2$, où l'on a $i=-1$, la congruence (26) se réduit à $a+b'\equiv 0$ (mod. p); il en résulte que l'expression générale des fonctions du deuxième ordre est

$$\theta z = \frac{az+b}{a'z-a};$$

on arrive au même résultat au moyen de la formule (10), puisqu'une fonction du deuxième ordre est égale à son inverse.

473. On voit, par les développements qui précèdent, que, pour former les différents groupes qui contiennent les puissances d'une même fonction linéaire pour le module premier p, il suffira de connaître une racine primitive de chacune des congruences

$$i^{p-1}\equiv 1,\quad i^{p+1}\equiv 1\quad (\text{mod. } p).$$

Les racines de la première ne sont autres que les racines primitives du nombre premier p, et l'on a vu au n° 372 comment on peut obtenir les racines primitives de la deuxième congruence. Veut-on, par exemple, former les

fonctions linéaires d'ordre $p+1$ pour les modules 5, 7, 11, il suffira de trouver une valeur de k pour chacun de ces modules. Or les racines primitives i sont données, pour ces différents cas, par les congruences

$$\frac{(i^6-1)(i-1)}{(i^3-1)(i^2-1)} \equiv 0 \quad (\text{mod. } 5),$$

$$\frac{i^8-1}{i^4-1} \equiv 0 \quad (\text{mod. } 7),$$

$$\frac{(i^{12}-1)(i^2-1)}{(i^6-1)(i^4-1)} \equiv 0 \quad (\text{mod. } 11),$$

ou

$$i^2 - i + 1 \equiv 0 \quad (\text{mod. } 5),$$

$$i^2 \pm 4i + 1 \equiv 0 \quad (\text{mod. } 7),$$

$$i^2 \pm 6i + 1 \equiv 0 \quad (\text{mod. } 11);$$

on a donc $k = 2$ pour le module 5, $k = \pm 2$ pour le module 7, et $k = \pm 3$ pour le module 11.

Des fonctions analytiques propres à représenter les substitutions.

474. Dans la plupart des cas où l'on a à considérer les substitutions de plusieurs quantités données, il convient de représenter ces quantités, comme nous avons déjà eu l'occasion de le faire, par une même lettre affectée d'un indice variable z susceptible de prendre un nombre de valeurs distinctes, égal au nombre n des quantités données. Alors les substitutions qu'on doit exécuter portent sur les indices.

Attribuons successivement à z les n valeurs dont cet indice est susceptible, et supposons qu'une fonction donnée $f(z)$ de z prenne en même temps les mêmes valeurs, abstraction faite de l'ordre ; on exécutera sur les quantités données une certaine substitution en y rem-

plaçant chaque indice z par $f(z)$. Cette substitution pourra être représentée par

$$\begin{bmatrix} f(z) \\ z \end{bmatrix},$$

ou plus simplement par $f(z)$.

Toute substitution peut ainsi être représentée analytiquement par le moyen d'une fonction; supposons, par exemple, que les valeurs de l'indice z soient les n nombres

$$0, 1, 2, \ldots, (n-1),$$

et que ces mêmes nombres soient dans un ordre différent.

$$a, b, c, \ldots, k;$$

si l'on fait, pour abréger,

$$F(z) = z(z-1)(z-2)\ldots(z-n+1),$$

et qu'on désigne par $F'(z)$ la dérivée de $F(z)$, la fonction entière

$$f(z) = \frac{aF(z)}{zF'(0)} + \frac{bF(z)}{(z-1)F'(1)} + \ldots + \frac{kF(z)}{(z-n+1)F'(n-1)}$$

prendra les valeurs $a, b, c, \ldots, k$, quand on donnera à z les valeurs $0, 1, 2, \ldots, (n-1)$; en conséquence, elle sera propre à représenter une substitution.

475. Lorsque le nombre n des quantités données est égal à un nombre premier p, il y a souvent avantage à prendre pour indices un système de p nombres entiers quelconques incongrus suivant le module p, et à regarder deux nombres congrus suivant le module comme pouvant indifféremment représenter le même indice. Alors la fonction représentée par $F(z)$ au numéro précédent se réduit à

$$F(z) = z^p - z,$$

t l'on a

$$F'(z) \equiv -1 \pmod{p}.$$

n même temps l'expression des fonctions entières $f(z)$, ropres à représenter les substitutions, devient

$$(z) \equiv -\frac{a(z^p - z)}{z} - \frac{b(z^p - z)}{z-1} - \ldots - \frac{k(z^p - z)}{z - p + 1} \pmod{p},$$

u, en effectuant les divisions,

$$\left.\begin{array}{l} (z) \equiv -a(z^{p-1} - 1) - b(z^{p-1} + z^{p-2} + \ldots + z) \\ \quad - c(z^{p-1} + 2z^{p-2} + \ldots + 2^{p-2}z) \ldots\ldots \\ \quad - k[z^{p-1} + (p-1)z^{p-2} + \ldots + (p-1)^{p-2}z] \end{array}\right\} \pmod{p}.$$

omme on a

$$a + b + c + \ldots + k \equiv 0 \pmod{p},$$

n peut écrire, en ordonnant par rapport à z,

$$\left.\begin{array}{l} (z) \equiv a - [b + 2^{p-2}c + \ldots + (p-1)^{p-2}k]z \\ \quad - [b + 2^{p-3}c + \ldots + (p-1)^{p-3}k]z^2 \\ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \quad - [b + 2c \quad + \ldots + (p-1)k]z^{p-2} \end{array}\right\} \pmod{p}.$$

476. Dans un article qui fait partie du tome LVII des *Comptes rendus de l'Académie des Sciences*, M. Hermite a démontré que les polynômes $f(z)$ dont nous enons de donner l'expression possèdent une propriété ui peut servir à les caractériser. On a effectivement ce héorème :

THÉORÈME. — *Soient $f(z)$ une fonction entière de z, coefficients entiers et du degré $p-2$, et $f_m(z)$ la fonction entière obtenue en rabaissant au-dessous de p, à aide de la congruence $z^p \equiv z$ (mod. p), le degré de la uissance $m^{\text{ième}}$ du polynôme $f(z)$. Pour que la fonction*

$f(z)$ soit propre à représenter une substitution de p indices incongrus suivant le module premier p, il faut et il suffit que, dans chacune des fonctions

$$f_2(z),\quad f_3(z),\quad \ldots,\quad f_{p-2}(z),$$

le coefficient de z^{p-1} soit congru à zéro suivant le module p.

En effet, soit

$$(1)\qquad f(z) = A_0 + A_1 z + A_2 z^2 + \ldots + A_{p-2} z^{p-2};$$

élevons ce polynôme à la $m^{\text{ième}}$ puissance, et réduisons ensuite par le moyen de la congruence

$$z^p \equiv z \pmod{p};$$

on aura un résultat de la forme

$$(2)\quad [f(z)]^m \equiv f_m(z) \equiv A_0^{(m)} + A_1^{(m)} z + \ldots + A_{p-1}^{(m)} z^{p-1} \pmod{p}.$$

Posons en outre

$$(3)\qquad [f(0)]^m + [f(1)]^m + \ldots + [f(p-1)]^m = S_m;$$

si l'on donne à z, dans la formule (2), les valeurs

$$0,\ 1,\ 2,\ 3,\ \ldots,\ (p-1),$$

et qu'on ajoute les résultats, il viendra

$$(4)\qquad S_m \equiv - A_{p-1}^{(m)} \pmod{p};$$

car z^{p-1} est congru à zéro ou à 1, suivant que z est nul ou différent de zéro, et la somme $1^\mu + 2^\mu + \ldots + (p-1)^\mu$ est congrue à zéro si μ est inférieur à $p-1$.

Cela posé, supposons que $f(z)$ soit propre à représenter une substitution. Alors la formule (3) se réduit à

$$0^m + 1^m + 2^m + \ldots + (p-1)^m \equiv S_m \pmod{p},$$

et par suite S_m est congrue à zéro suivant le module p,

pour toutes les valeurs de m inférieures à $p-1$; on a donc, par la formule (4),

(5) $$A_{p-1}^{(m)} \equiv 0 \pmod{p}.$$

En second lieu, supposons la fonction $f(z)$ telle, que la congruence (5) ait lieu pour les valeurs 2, 3, ..., $(p-2)$ de m. On aura par la formule (4)

$$S_m \equiv 0 \pmod{p},$$

pour les mêmes valeurs de m; cette congruence subsistera aussi pour $m=1$, d'après la formule (1), et pour $m=p$, puisque $z^p \equiv z$ quel que soit z. On voit alors, en se reportant aux formules de Newton, que la congruence

$$[Z-f(0)][Z-f(1)]\ldots[Z-f(p-1)] \equiv 0 \pmod{p}$$

a la forme

$$Z^p - \alpha Z \equiv 0 \pmod{p},$$

ou même la forme

$$Z^p - Z \equiv 0 \pmod{p};$$

effectivement, toute valeur de α autre que 1 ou zéro ne laisserait subsister qu'une seule racine réelle Z qui serait égale à zéro; la valeur $\alpha = 0$ donnerait p racines nulles, ce qui est inadmissible, car la congruence

$$f(z) \equiv 0 \pmod{p},$$

étant du degré $p-2$, ne peut avoir plus de $p-2$ racines.

Il résulte de là que, si l'on donne à z les valeurs

$$0,\ 1,\ 2,\ \ldots,\ (p-1),$$

la fonction $f(z)$ prend successivement les mêmes valeurs, abstraction faite de l'ordre; elle est donc propre à représenter une substitution.

477. Si la fonction entière $f(z)$ représente une substitution de p indices incongrus suivant le module premier p, il est évident que la fonction

$$\theta z = \alpha f(z + 6) + \gamma$$

représentera aussi une substitution. Or on peut disposer de l'indéterminée α, de manière à réduire à l'unité le coefficient de la plus haute puissance de z; l'indéterminée 6 permet ensuite de faire disparaître la puissance de z immédiatement inférieure; enfin on peut disposer de γ de manière à faire évanouir le terme indépendant de z. La fonction θz aura alors la forme

$$\theta z = a_1 z + a_2 z^2 + \ldots + a_{\nu-2} z^{\nu-2} + z^\nu,$$

ν étant égal ou inférieur à $p - 2$.

M. Hermite a donné aux substitutions de la forme θz le nom de *substitutions réduites;* il est clair que ces substitutions en fourniront d'autres plus générales, $f(z)$, au moyen de la formule

$$f(z) = \alpha\theta(z + 6) + \gamma,$$

où α, 6, γ désignent des indéterminées. Il faut remarquer que les substitutions réduites ne déplacent pas l'indice zéro.

Le théorème du n° 476 prend une forme plus simple quand on l'applique aux fonctions réduites. Effectivement, si l'on élève la fonction θz à la puissance de degré m, et qu'on réduise au moyen de la congruence $z^p \equiv z$ (mod. p), on n'introduira aucun terme indépendant de z; si donc on remplace ensuite z^{p-1} par 1, le coefficient de z^{p-1} deviendra le terme indépendant de z. On peut alors énoncer comme il suit le théorème établi plus haut :

Pour que la fonction réduite θz puisse représenter

une substitution, il faut et il suffit qu'en élevant θz aux puissances 2, 3, ..., $(p-2)$, et en réduisant les résultats par la congruence $z^{p-1}\equiv 1$ (mod. p), les termes indépendants de z soient congrus à zéro.

Les fonctions réduites θz sont encore susceptibles d'une réduction ultérieure, car, si l'on pose

$$\Theta(z) = a\,\theta(\alpha z),$$

on pourra disposer de l'indéterminée α de manière à réduire à l'unité le coefficient de la plus haute puissance de z, dans $\Theta(z)$, et il restera une indéterminée a dont on pourra disposer à volonté. Ces considérations trouveront plus loin leur application.

478. Lorsque le nombre n des quantités données est égal à une puissance p^ν d'un nombre premier, on peut choisir pour indices, avec Galois, les p^ν valeurs que peut prendre l'expression

$$a_0 + a_1 i + a_2 i^2 + \ldots + a_{\nu-1} i^{\nu-1},$$

dans laquelle i désigne une racine d'une congruence irréductible

$$F(x) \equiv 0 \quad (\text{mod. } p)$$

du degré ν. Si la fonction irréductible $F(x)$ appartient à l'exposant $p^\nu - 1$, i sera une racine primitive pour la congruence

$$x^{p^\nu-1} - 1 \equiv 0 \quad (\text{mod. } p)$$

et les indices autres que zéro seront représentés par les puissances

$$i,\ i^2,\ \ldots,\ i^{p^\nu-1}.$$

Enfin, lorsque le nombre n est un nombre composé,

$$n = p^\nu q^\mu r^\lambda \ldots,$$

$p, q, r, \ldots$ étant des nombres premiers, et $\nu, \mu, \lambda, \ldots$ des exposants quelconques, il peut être avantageux de représenter les quantités données par une même lettre affectée de plusieurs indices $\alpha, \beta, \gamma, \ldots$, en nombre égal à celui des nombres premiers $p, q, r, \ldots$, et de prendre pour valeurs des indices les fonctions entières composées respectivement avec une racine des congruences

$$\begin{aligned} F_1(x) &\equiv 0 \pmod{p},\\ F_2(x) &\equiv 0 \pmod{q},\\ F_3(x) &\equiv 0 \pmod{r},\\ &\ldots\ldots\ldots\ldots, \end{aligned}$$

$F_1(x), F_2(x), F_3(x), \ldots$ désignant des fonctions entières des degrés $\nu, \mu, \lambda, \ldots$, irréductibles relativement à leurs modules respectifs $p, q, r, \ldots$.

Des substitutions rationnelles et linéaires.

479. Les fonctions entières et linéaires $az + b$, prises suivant le module premier p, donnent des substitutions des p indices

$$0,\ 1,\ 2,\ \ldots,\ (p-1).$$

Le nombre total de ces substitutions est $p(p-1)$, et il est évident qu'elles forment un système conjugué.

Les fonctions rationnelles de la forme

$$(1)\qquad \theta z = \frac{az+b}{a'z+b'},$$

prises suivant le module premier p, peuvent être employées pour représenter des substitutions de $p+1$ indices; les valeurs qu'il faut attribuer à ces indices sont alors

$$0,\ 1,\ 2,\ \ldots,\ (p-1),\ \infty,$$

et l'on doit toujours regarder deux nombres congrus suivant le module p comme pouvant représenter le même indice. La substitution de l'infini à z se fait d'après les règles de l'Algèbre ordinaire, et lorsque, pour une valeur particulière de z, le dénominateur θz est congru à zéro, la fonction prend la valeur de ∞. C'est là une convention qu'on est libre de faire, attendu qu'elle n'est en contradiction avec aucun des principes fondamentaux de la théorie des congruences.

En résolvant la formule (1) par rapport à z, il vient

$$z = \frac{b - b'\theta z}{a'\theta z - a};$$

cette formule montre qu'il n'existe qu'une seule valeur de z propre à faire acquérir à θz une valeur donnée, ce qui est nécessaire pour que θz puisse représenter une substitution.

La congruence

$$(2) \qquad \theta z \equiv z \pmod{p}$$

peut se mettre sous la forme

$$(3) \qquad a'z^2 - (a - b')z - b \equiv 0 \pmod{p},$$

ou

$$[2a'z - (a - b')]^2 \equiv (a + b')^2 - 4(ab' - ba') \pmod{p}.$$

Elle n'aura aucune racine réelle si la quantité

$$(4) \qquad (a + b')^2 - 4(ab' - ba')$$

est non-résidu quadratique relativement à p; alors, la congruence (2) ne pouvant subsister pour aucune valeur de z, la substitution θz déplace tous les indices. Si la quantité (4) est congrue à zéro, la congruence (2) ou (3) a deux racines réelles et égales; par conséquent, la sub-

stitution θz déplace p indices. Enfin, si l'expression (4) est résidu quadratique de p, la congruence (2) a deux racines réelles et inégales; en conséquence, la substitution θz ne déplace que $p-1$ indices.

480. Désignons par n l'ordre de la fonction linéaire θz, et considérons la suite

$$z,\ \theta z,\ \theta^2 z,\ \ldots,\ \theta^{n-1} z.$$

Si la congruence $\theta z \equiv z \pmod{p}$ a une racine réelle z_0, les termes de la suite précédente se réduiront tous à z_0 pour $z = z_0$; mais, pour toute autre valeur z_1 de z, aucun de ces termes ne se réduira à z_0. Laissant de côté ces valeurs z_0 s'il en existe, je dis que les termes de la suite précédente auront toujours des valeurs distinctes; car si l'on avait, par exemple,

$$\theta^{\mu+\nu} z_1 \equiv \theta^{\mu} z_1 \pmod{p},$$

en posant

$$z_2 = \theta^{\mu} z_1,$$

il en résulterait

$$\theta^{\nu} z_2 \equiv z_2 \pmod{p};$$

ce qui est impossible, car, ν étant inférieur à n, on ne peut avoir identiquement

$$\theta^{\nu} z \equiv z \pmod{p};$$

d'ailleurs, par les formules du n° 467, la précédente congruence n'est autre chose que

$$\theta z \equiv z \pmod{p},$$

et, en conséquence, elle n'admet pas la racine z_2.

On peut conclure de là que la fonction linéaire θz représente une substitution d'ordre n, et, d'après la classification que nous avons établie, on voit que le système

des substitutions linéaires ne comprend que des substitutions circulaires, dont l'ordre est l'un des nombres $p+1$, p, $p-1$ avec les puissances des mêmes substitutions.

Le nombre total des substitutions linéaires est $(p+1)p(p-1)$, et parmi ces substitutions il y en a $\frac{(p+1)p(p-1)}{2}$ dont le *déterminant* est résidu quadratique du module. De là résulte la proposition suivante :

Théorème. — *L'ensemble de toutes les substitutions linéaires, relatives à un module premier p, constitue un système conjugué trois fois transitif d'ordre $(p+1)p(p-1)$. En outre, les substitutions linéaires dont le déterminant est résidu quadratique forment un système conjugué deux fois transitif d'ordre $\frac{1}{2}(p+1)p(p-1)$.*

Effectivement, le premier de ces systèmes renferme des substitutions circulaires d'ordre $p+1$, d'ordre p et d'ordre $p-1$. Quant au second système, il renferme des substitutions circulaires d'ordre p avec des substitutions régulières d'ordre $\frac{p\pm 1}{2}$, et parmi ces dernières on en peut toujours trouver une qui remplace un indice donné z_0 par un autre indice donné z_1.

Dans le cas de $p=5$, on retrouve immédiatement le système triplement transitif de substitutions de six lettres dont nous nous sommes occupé au n° 452.

De quelques propriétés des substitutions linéaires.

481. Théorème I. — *Si* Ez *désigne généralement les $p(p-1)$ substitutions linéaires et entières, relati-*

vement au module p, et que φz soit une fonction linéaire quelconque donnée, les substitutions de la forme $\varphi^{-1}E\varphi z$ formeront un système conjugué d'ordre $p(p-1)$ qui ne déplaceront pas l'indice z pour lequel la fonction φz est infinie.

En effet, en premier lieu, les substitutions $\varphi^{-1}E\varphi z$ forment un système conjugué semblable à celui des substitutions Ez (n° 427). En second lieu, soit z_0 l'indice que les substitutions $\varphi^{-1}E\varphi z$ laissent immobile ; on aura

$$\varphi^{-1}E\varphi z_0 \equiv z_0 \pmod{p},$$

d'où

$$E\varphi z_0 \equiv \varphi z_0 \pmod{p}.$$

Il résulte de là que les substitutions Ez ne déplacent pas l'indice φz_0 ; on a donc

$$\varphi z_0 = \infty.$$

Corollaire I. — *Il existe $p+1$ systèmes conjugués d'ordre $p(p-1)$ dont chacun est composé de substitutions linéaires qui toutes laissent immobile un même indice.*

Corollaire II. — *Chaque système d'ordre $p(p-1)$ s'obtient en multipliant l'un par l'autre les systèmes formés respectivement par les puissances de deux substitutions linéaires qui ne déplacent pas un même indice z_0, et qui sont l'une d'ordre p, l'autre de l'ordre $p-1$.*

Car soient

$$z,\ \theta z,\ \theta^2 z,\ \ldots,\ \theta^{p-2} z,\ \theta^{p-1} z,$$
$$z,\ \varphi z,\ \varphi^2 z,\ \ldots,\ \varphi^{p-2} z$$

les systèmes formés par les puissances des substitutions θz et φz des ordres respectifs p et $p-1$, qui ne déplacent pas un indice z_0. Le nombre des produits $\varphi^\mu \theta^\nu z$ étant

$p(p-1)$, il suffit de montrer que ces produits sont distincts. Or, si l'on avait

$$\varphi^\mu \theta^\nu z = \varphi^{\mu'} \theta^{\nu'} z,$$

on en conclurait

$$\varphi^{\mu-\mu'} z = \theta^{\nu'-\nu} z,$$

ce qui exige que l'on ait $\mu' = \mu$, $\nu' = \nu$, puisque la substitution φz d'ordre $p-1$ laisse deux indices immobiles, tandis que θz déplace p indices. Notre proposition est donc établie.

Corollaire III. — *Le système des* $(p+1)p(p-1)$ *substitutions linéaires s'obtient en multipliant l'un des systèmes d'ordre* $p(p-1)$, *dont les substitutions laissent un indice immobile, par le système des puissances d'une substitution linéaire d'ordre* $p+1$.

Soient

$$z, \ \varphi_1 z, \ \varphi_2 z, \ \ldots, \ \varphi_{p(p-1)-1} z$$

et

$$z, \ \theta z, \ \theta^2 z, \ \ldots, \ \theta^p z$$

les deux systèmes dont il s'agit. Les produits $\varphi_\mu \theta^\nu z$ étant au nombre de $(p+1)p(p-1)$, il suffit d'établir qu'ils sont distincts. Or, si μ' et ν' ne sont pas égaux respectivement à μ et ν, on ne peut pas avoir

$$\varphi_{\mu'} \theta^{\nu'} z = \varphi_\mu \theta^\nu z,$$

car il en résulterait

$$\varphi_\mu^{-1} \varphi_{\mu'} z = \theta^{\nu-\nu'} z,$$

ce qui est impossible, puisque la substitution θ déplace un indice que les substitutions φ laissent immobile.

482. Théorème II. — *Soient* θz *une substitution linéaire d'ordre* p *qui ne déplace pas l'indice* z_0, *et* φz

une substitution linéaire quelconque. Pour que l'on puisse avoir

$$\varphi^{-1}\theta\varphi z = \theta^{\mu} z,$$

il faut et il suffit que la substitution φz ne déplace pas l'indice z_0.

En effet, la congruence

$$\theta z_0 \equiv z_0 \pmod{p}$$

entraîne

$$\theta^{\mu} z_0 \equiv z_0 \pmod{p}.$$

Si donc on a

$$\theta\varphi z = \varphi\theta^{\mu} z,$$

il viendra, pour $z = z_0$,

$$\theta\varphi z_0 \equiv \varphi z_0 \pmod{p},$$

et, puisque la substitution θz déplace tous les indices à l'exception de z_0, on a

$$\varphi z_0 \equiv z_0 \pmod{p},$$

ce qui exprime que la substitution φz laisse z_0 immobile.

Réciproquement, si φz ne déplace pas z_0, il en sera de même de la substitution $\varphi^{-1}\theta\varphi z$; celle-ci est d'ailleurs du même ordre que θz. Donc les deux congruences

$$\theta z \equiv z, \quad \varphi^{-1}\theta\varphi z \equiv z \pmod{p}$$

ont l'une et l'autre la même racine unique z_0; il en résulte, d'après le mode de formation des fonctions linéaires, que les fonctions $\varphi^{-1}\theta\varphi z$ et θz font partie d'un même groupe de puissances, et l'on a

$$\varphi^{-1}\theta\varphi z = \theta^{\mu} z.$$

Il faut remarquer que l'ordre n de φz est égal à p ou à un diviseur de $p-1$. Mais, si le premier cas a lieu, φz n'est autre chose qu'une puissance de θz.

Corollaire I. — *Une substitution linéaire d'ordre p n'est échangeable avec aucune autre substitution linéaire, si ce n'est avec ses puissances.*

En effet, si la substitution θz est d'ordre p et que φz ne soit pas une puissance de θz, l'égalité

$$(1) \qquad \theta\varphi z = \varphi\theta z \quad \text{ou} \quad \varphi^{-1}\theta\varphi z = \theta z$$

exige, comme nous venons de le dire, que l'ordre de φz soit un diviseur de $p-1$. Alors la congruence

$$(2) \qquad \varphi z \equiv z \pmod{p}$$

a une racine z_1 distincte de z_0, et l'égalité (1) donne, pour $z = z_1$,

$$\theta z_1 \equiv \varphi\theta z_1 \pmod{p},$$

d'où il suit que la congruence (2) a la racine θz_1. Or les racines de cette congruence sont z_1 et $z_0 = \theta z_0$; donc il faudrait que l'on eût

$$\theta z_1 \equiv z_1 \quad \text{ou} \quad \theta z_1 \equiv \theta z_0,$$

et, par suite, $z_1 = z_0$, ce qui n'a pas lieu.

Corollaire II. — *Soient θz une substitution linéaire d'ordre p et φz une substitution linéaire dont l'ordre n est un diviseur de $p-1$. Si les substitutions θz et φz laissent immobile un même indice z_0, on obtiendra un système de substitutions conjuguées d'ordre np en multipliant le système des puissances de θz par celui des puissances de φz. En outre, ce système d'ordre np renfermera toutes les substitutions linéaires d'ordre n qui ne déplacent pas l'indice z_0.*

Il est évident qu'on obtiendra un système conjugué d'ordre np en multipliant l'un par l'autre les deux sys-

tèmes

$$z,\ \theta z,\ \theta^2 z,\ \ldots,\ \theta^{p-1} z,$$
$$z,\ \varphi z,\ \varphi^2 z,\ \ldots,\ \varphi^{n-1} z.$$

En outre, ce système d'ordre np renferme toutes les substitutions d'ordre n de la forme $\theta^{-i}\varphi\theta^i z$, et, comme i peut avoir l'une quelconque des valeurs

$$0,\ 1,\ 2,\ 3,\ \ldots,\ (p-1),$$

on trouvera p systèmes formés chacun par les puissances d'une substitution d'ordre n qui ne déplace pas l'indice z_0. Or il n'existe pas un plus grand nombre de tels systèmes : il suffit donc d'établir que ceux dont nous venons de parler sont distincts. Je dis que l'égalité

$$\theta^{-i}\varphi\theta^i z = \theta^{-i-j}\varphi^k\theta^{i+j}$$

est impossible, car, si elle avait lieu, il en résulterait

$$\theta^j\varphi\theta^{-j} z = \varphi^k z;$$

mais on a $\varphi^{-1}\theta\varphi z = \theta^\mu z$, et, par conséquent,

$$\varphi^{-1}\theta^j\varphi z = \theta^{\mu j} z,\quad \theta^j\varphi z = \varphi\theta^{\mu j} z:$$

on aurait donc

$$\varphi\theta^{(\mu-1)j} z = \varphi^k z,\quad \theta^{(\mu-1)j} z = \varphi^{k-1} z,$$

ce qui exige $k=1$, $\mu=1$. Mais, si l'on avait $\mu=1$, les substitutions θz et φz seraient échangeables, ce qui n'a pas lieu.

483. Théorème III. — *Soient θz une substitution linéaire d'ordre $p\pm 1$, et φz une substitution linéaire distincte des puissances de θz. Pour que l'on puisse avoir*

(1) $$\varphi^{-1}\theta\varphi z = \theta^\mu z,$$

il faut et il suffit que φz soit une substitution du deuxième

ordre et que les racines réelles ou imaginaires z_0, z_1 *de la congruence*

$$\theta z \equiv z \pmod{p}$$

soient telles, que l'on ait

$$\varphi z_0 \equiv z_1, \quad \varphi z_1 \equiv z_0 \pmod{p}.$$

Dans le cas où l'ordre de θz *est* $p-1$, *les racines* z_0, z_1 *sont réelles et la dernière condition exprime que la substitution* φz *transpose les deux indices que* θz *laisse immobiles.*

Si l'égalité (1) a lieu, le système des puissances de $\varphi^{-1}\theta\varphi z$, savoir

(2) $$z,\ \varphi^{-1}\theta\varphi z,\ \varphi^{-1}\theta^2\varphi z,\ \ldots,$$

coïncide avec le système

(3) $$z,\ \theta z,\ \theta^2 z,\ \ldots$$

des puissances de θz. Chacun des systèmes (2) et (3) renferme une substitution du deuxième ordre, et alors ces deux substitutions doivent être égales; on a ainsi

(4) $$\varphi^{-1}\theta^{\frac{p\pm 1}{2}}\varphi z = \theta^{\frac{p\pm 1}{2}} z \quad \text{ou} \quad \theta^{\frac{p\pm 1}{2}}\varphi z = \varphi\theta^{\frac{p\pm 1}{2}} z.$$

Réciproquement, si cette égalité (4) a lieu, les systèmes (2) et (3) étant du même ordre $p\pm 1$ et ayant une substitution commune, ils coïncident nécessairement.

Si l'on remplace z par $\theta^{\frac{p\pm 1}{2}}\varphi z$, l'égalité (4) devient

$$\theta^{\frac{p\pm 1}{2}}\varphi\theta^{\frac{p\pm 1}{2}}\varphi z = \varphi\theta^{p\pm 1}\varphi z = \varphi^2 z;$$

$\theta^{\frac{p\pm 1}{2}}\varphi z$ et φz ont donc le même carré, et il en résulte que ces fonctions sont du deuxième ordre. En effet, si le contraire avait lieu, les deux substitutions dont il s'agit

appartiendraient l'une et l'autre au groupe des puissances d'une même substitution linéaire ψz; on aurait

$$\theta^{\frac{p\pm1}{2}}\varphi z = \psi^{\mu} z, \quad \varphi z = \psi^{\nu} z,$$

d'où

$$\theta^{\frac{p\pm1}{2}} z \equiv \psi^{\mu-\nu} z,$$

et par suite les fonctions φ et θ feraient partie du même groupe de puissances, ce qui est contre l'hypothèse. Ainsi l'on a

$$(5)\qquad \varphi^2 z = z, \quad \theta^{\frac{p\pm1}{2}}\varphi\theta^{\frac{p\pm1}{2}}\varphi z = z,$$

et réciproquement ces égalités entraînent la formule (4).

Cela posé, soient z_0 et z_1 les racines réelles ou imaginaires des congruences

$$\theta z \equiv z, \quad \theta^{\frac{p\pm1}{2}} z \equiv z \pmod{p},$$

l'égalité (4) donnera

$$\varphi^{-1}\theta^{\frac{p\pm1}{2}}\varphi z_0 \equiv z_0, \quad \varphi^{-1}\theta^{\frac{p\pm1}{2}}\varphi z_1 \equiv z_1 \pmod{p},$$

ou

$$\theta^{\frac{p\pm1}{2}}\varphi z_0 \equiv \varphi z_0, \quad \theta^{\frac{p\pm1}{2}}\varphi z_1 \equiv \varphi z_1 \pmod{p},$$

d'où il suit que φz_0 et φz_1 ne sont autre chose que z_0 et z_1. Mais si l'on a $\varphi z_0 \equiv z_0$, $\varphi z_1 \equiv z_1$, les fonctions φz et $\theta^{\frac{p\pm1}{2}} z$, qui sont du deuxième ordre, coïncideront; donc on a

$$(6)\qquad \varphi z_0 \equiv z_1, \quad \varphi z_1 \equiv z_0 \pmod{p}.$$

Réciproquement, si ces congruences (6) ont lieu, les congruences du deuxième degré

$$\varphi^{-1}\theta^{\frac{p\pm1}{2}}\varphi z \equiv z, \quad \theta^{\frac{p\pm1}{2}} z \equiv z \pmod{p},$$

auront les mêmes racines, et, comme leurs premiers membres sont des fonctions du deuxième ordre, ces premiers membres seront égaux entre eux.

Corollaire I. — *Il existe $p \pm 1$ substitutions du deuxième ordre φz telles, que l'on ait*

$$\varphi^{-1}\theta\varphi z = \theta^{\lambda} z,$$

savoir : $p+1$ si θz est de l'ordre $p+1$, et $p-1$ si θz est de l'ordre $p-1$.

En effet, z_0 et z_1 désignant comme précédemment les racines de la congruence $\theta z \equiv z \pmod{p}$, si l'on a

$$\varphi z_0 \equiv z_1, \quad \varphi z_1 \equiv z_0 \pmod{p},$$

la fonction linéaire du deuxième ordre φz sera

$$\varphi z = \frac{a(z - z_0 - z_1) + a' z_0 z_1}{a' z - a};$$

cette expression renferme une indéterminée $\frac{a}{a'}$ à laquelle on peut attribuer les $p+1$ valeurs

$$0, 1, 2, 3, \ldots, (p-1), \infty;$$

toutefois, quand z_0 et z_1 sont réelles, il faut rejeter les deux valeurs $\frac{a}{a'} = z_0$, $\frac{a}{a'} = z_1$ pour lesquelles l'expression de φz se réduit à une constante. Donc le nombre des substitutions φz est toujours égal à l'ordre de θz.

Corollaire II. — *Si θz est une substitution d'ordre $p \pm 1$ et que φz soit l'une des $p \pm 1$ substitutions du deuxième ordre telles, que*

$$\varphi^{-1}\theta\varphi z = \theta^{\lambda} z,$$

on obtiendra un système de $2(p \pm 1)$ substitutions conju-

guées, en joignant aux puissances de θz leurs produits par φz. En outre, ces $p \pm 1$ produits seront précisément les $p \pm 1$ substitutions du deuxième ordre qui satisfont à la précédente égalité.

D'abord il est évident qu'on obtiendra un système conjugué, en multipliant l'un par l'autre, à droite ou à gauche, les deux systèmes

$$z,\ \theta z,\ \theta^2 z,\ \ldots,\ \theta^{(p\pm 1)-1} z,$$
$$z,\ \varphi z.$$

Ensuite, si l'on considère un des produits obtenus,

(1) $$\psi z = \theta^i \varphi z,$$

comme l'égalité

$$\varphi^{-1}\theta\varphi z = \theta^\mu z$$

entraîne

$$\varphi^{-1}\theta^i\varphi z = \theta^{\mu i} z,$$

on aura aussi

(2) $$\psi z = \varphi\theta^{\mu i} z.$$

Les formules (1) et (2) donnent

$$\psi^2 z = \theta^i\varphi\varphi\theta^{\mu i} z = \theta^{(\mu+1)i} z;$$

cela exige que l'on ait

$$\psi^2 z = z,$$

car autrement les fonctions ψ et φ appartiendraient au groupe des puissances de θ, ce qui est contre l'hypothèse. Les produits $\theta^i\varphi z$ sont donc tous du deuxième ordre.

L'égalité (1) donne

$$\theta^i z = \psi\varphi z,$$

et il en résulte que toute substitution linéaire θz est le produit de deux substitutions du deuxième ordre.

Remarque. — On obtient un système conjugué d'ordre $2n$ si, en posant $p \pm 1 = mn$, on multiplie l'un par l'autre les deux systèmes

$$z,\ \theta^m z,\ \theta^{2m} z,\ \ldots,\ \theta^{(n-1)m} z,$$

$$z,\ \varphi z.$$

Corollaire III. — *Pour que deux substitutions linéaires qui ne sont pas des puissances d'une même substitution soient échangeables, il faut et il suffit qu'elles soient toutes deux du deuxième ordre, et que les indices (réels ou imaginaires) que l'une des substitutions laisse immobiles soient transposés par l'autre substitution.*

En effet, soient φ et ψ deux substitutions linéaires qui ne sont pas des puissances d'une même substitution. Si ces substitutions sont échangeables, aucune d'elles ne sera d'ordre p (n° **482**); ψz sera donc une puissance d'une substitution θz d'ordre $p \pm 1$. L'égalité

$$\psi\varphi z = \varphi\psi z \quad \text{ou} \quad \varphi^{-1}\psi\varphi z = \psi z$$

ne peut avoir lieu que si le groupe des puissances de $\varphi^{-1}\theta\varphi z$ coïncide avec celui des puissances de θz; cela exige que φz soit du deuxième ordre. Le même raisonnement prouve que ψz est aussi du deuxième ordre; alors, d'après le théorème qui précède, si z_0 et z_1 désignent les racines de la congruence $\varphi z \equiv z \pmod{p}$, les conditions pour que φz et ψz soient échangeables sont

$$\psi z_0 \equiv z_1, \quad \psi z_1 \equiv z_0 \pmod{p};$$

il est évident que l'une de ces conditions entraîne l'autre.

484. Théorème IV. — *Soient θz une substitution linéaire d'ordre $p+1$, pour le module p, et ϖz une substitution linéaire quelconque. On pourra satisfaire à*

l'égalité

$$\theta^m \varpi \theta^n z = \mathrm{E}z,$$

ou Ez *désigne une substitution linéaire et entière, en attribuant à l'un quelconque des nombres m et n l'une quelconque des valeurs* 0, 1, 2, 3, ..., p; *la valeur de l'autre nombre sera alors déterminée.*

En effet, la substitution θz étant d'ordre $p+1$, les puissances

$$z,\quad \theta z,\quad \theta^2 z,\quad \ldots,\quad \theta^p z$$

prendront dans un certain ordre les valeurs

$$0,\ 1,\ 2,\ 3,\ \ldots,\ (p-1),\ \infty,$$

quelle que soit la valeur que l'on attribue à z. Cela étant, posons

$$\theta^n \infty = z_0,\quad \varpi z_0 = z_1,\quad \theta^m z_1 = \infty.$$

Si le nombre n est donné, la première de ces formules détermine z_0, la deuxième donne ensuite z_1, et alors le nombre m est déterminé par la troisième formule. Si au contraire le nombre m est donné, la troisième formule détermine z_1, après quoi la deuxième donne $z_0 = \varpi^{-1} z_1$ et le nombre n est ensuite déterminé par la première formule. D'après cela on a

$$\theta^m \varpi \theta^n \infty = \infty,$$

c'est-à-dire que la fonction linéaire $\theta^m \varpi \theta^n z$ devient infinie pour $z = \infty$, et par conséquent elle est entière.

Corollaire. — *Si le déterminant de la substitution* ϖz *est résidu quadratique du module* p, *que* r *désigne une racine primitive pour ce module et que les entiers* m, n *soient tels, que la substitution*

$$\theta^{p+1-m} \varpi \theta^n z$$

soit entière; si l'on pose en outre

$$f_{2\mu} z = \theta^{2\mu} z,\quad f_{2\mu+1} z = \theta^{2\mu+1}(rz),$$

la substitution

$$f_m^{-1} \varpi f_n z$$

sera entière et son déterminant sera résidu quadratique de p.

En effet, suivant que m et n sont pairs ou impairs, la substitution dont il s'agit a l'une des formes

$$\theta^{-m} \varpi \theta^n z, \quad \theta^{-m} \varpi \theta^n rz, \quad \frac{1}{r} \theta^{-m} \varpi \theta^n z, \quad \frac{1}{r} \theta^{-m} \varpi \theta^n rz;$$

elle est donc entière. D'ailleurs son déterminant est résidu quadratique de p, car elle est le produit de trois substitutions $f_m^{-1} z$, ϖz, $f_n z$, dont les déterminants sont résidus quadratiques.

Exemple. — Supposons $p = 7$, $r = 3$, et prenons

$$\theta z = \frac{z+6}{z+4}, \quad \varpi z = \frac{z+2}{z+6},$$

on aura

$$\frac{1}{3} \theta^7 \varpi \theta^0 z = z, \qquad \theta^2 \varpi \theta^4 z = 4z + 4,$$

$$\theta^0 \varpi \theta\, 3z = z, \qquad \frac{1}{3} \theta \varpi \theta^5 3z = 2z + 6,$$

$$\frac{1}{3} \theta^5 \varpi \theta^2 z = 4z + 4, \qquad \theta^4 \varpi \theta^6 z = z + 3,$$

$$\theta^6 \varpi \theta^3 3z = 2z + 6, \qquad \frac{1}{3} \theta^3 \varpi \theta^7 3z = 4z + 4.$$

Sur les substitutions de cinq et de sept lettres.

485. Lorsque le nombre premier p est égal à 3, les substitutions des $p-1$ indices z

$$0,\ 1,\ 2,\ 3,\ \ldots,\ (p-1)$$

sont toutes linéaires et entières.

M. Betti a donné pour le cas de cinq lettres l'expres-

sion analytique des substitutions, et M. Hermite a résolu ensuite le même problème à l'égard des substitutions de sept lettres. Nous allons exposer ici ces importants résultats.

DES SUBSTITUTIONS DE CINQ LETTRES — Considérons d'abord le cas de cinq indices; d'après ce qui a été dit au n° 477, les formes réduites des substitutions sont

$$\theta z \equiv z, \quad z^2, \quad z^3 + az \quad (\text{mod. } 5).$$

La deuxième forme doit être exclue, car on en tire

$$[\theta z]^2 \equiv z^4 \equiv 1 \quad (\text{mod. } 5);$$

la troisième donne

$$[\theta z]^2 \equiv z^6 + 2az^4 + a^2z^2 \equiv (1 + a^2)z^2 + 2a \quad (\text{mod. } 5),$$

et pour faire disparaître le terme indépendant il faut poser $a = 0$. Toutes les autres conditions se trouvant d'ailleurs remplies (n° 477) par l'expression $\theta z \equiv z^3$, il en résulte que la totalité des substitutions pour un système de cinq indices sont comprises dans les deux formes

$$\alpha z + 6, \quad \alpha(z + 6)^3 + \gamma,$$

où l'on n'excepte que la valeur de $\alpha = 0$.

486. DES SUBSTITUTIONS DE SEPT LETTRES. — Dans le cas de sept indices, les formes réduites ne peuvent être que les suivantes :

$$\left.\begin{array}{l}\theta z \equiv z, \quad z^2, \quad z^3 + az, \\ z^4 + az^2 + bz, \quad z^5 + az^3 + bz^2 + cz\end{array}\right\} \quad (\text{mod. } 7),$$

parmi lesquelles on doit rejeter d'abord la deuxième et la troisième, parce que le terme indépendant de z subsiste nécessairement dans le cube de l'une et dans le carré de l'autre.

Soit

$$\theta z \equiv z^4 + a z^2 + b z \pmod{7};$$

on voit immédiatement que le terme indépendant dans $[\theta z]^2$ est a; on a donc $a \equiv 0 \pmod{7}$. On trouve ensuite

$$\left.\begin{aligned}(z^4 + bz)^3 &= z^{12} + 3bz^9 + 3b^2z^6 + b^3z^3\\ &\equiv (b^2 + 3b)z^3 + (3b^2 + 1)\end{aligned}\right\} \pmod{7},$$

ce qui exige que l'on fasse

$$3b^2 + 1 \equiv 0, \quad b \equiv \pm 3 \pmod{7}.$$

On a ainsi les deux formes

$$\theta z = z^4 + 3z, \quad \theta z = z^4 - 3z;$$

mais la seconde se ramène à la première par la transformation indiquée au n° **477**, car, si l'on fait

$$\Theta z = a^2 \theta(az) = a^2(a^4 z^4 + 3az) = z^4 + 3a^3 z,$$

cette formule se réduit à

$$\Theta z = z^4 - 3z,$$

si l'on suppose

$$a^3 \equiv -1 \pmod{7},$$

c'est-à-dire si l'on prend a non-résidu quadratique de 7. Cela étant, on a la série des puissances qui suit :

$$\left.\begin{aligned}\theta z &\equiv z^4 + 3z\\ [\theta z]^2 &\equiv 6z^5 + 3z^2\\ [\theta z]^3 &\equiv z^3\\ [\theta z]^4 &\equiv 3z^4 + z\\ [\theta z]^5 &\equiv 3z^5 + 6z^2\end{aligned}\right\} \pmod{7},$$

en sorte que toutes les autres conditions se trouvent remplies d'elles-mêmes.

Soit en dernier lieu

$$\theta z \equiv z^5 + a z^3 + b z^2 + c z \pmod{7};$$

on aura, en égalant à zéro le terme indépendant de z dans le carré, dans le cube et dans la quatrième puissance de θz,

$$\left.\begin{array}{r} 2c + a^2 \equiv 0, \\ b(3 + 6ac + b^2) \equiv 0, \\ ab^2 + 4b^2c^2 + 2(2a + c^2)(1 + 2ac + b^2) \equiv 0 \end{array}\right\} \pmod{7}.$$

La deuxième condition est satisfaite en posant

$$b \equiv 0 \pmod{7},$$

ce qui réduit la troisième à

$$(2a + c^2)(1 + 2ac) \equiv 0 \pmod{7};$$

remplaçant c par la valeur $-\frac{1}{2}a^2 \equiv 3a^2 \pmod{7}$, tirée de la première congruence, on obtient l'identité

$$2(a + a^4)(1 - a^3) \equiv 2(a - a^7) \equiv 0 \pmod{7}.$$

On a ainsi cette expression

$$\theta z \equiv z^5 + az^3 + 3a^2 z \pmod{7},$$

où a reste indéterminé, mais que l'on peut ramener au cas de $a \equiv 0$ et à ceux de $a \equiv 1$, $a \equiv 3$, au moyen de la relation

$$\alpha\theta(\alpha z) \equiv z^5 - a\alpha^4 z^3 + 3a^2\alpha^2 z \pmod{7}.$$

On vérifie facilement que la cinquième puissance de notre expression de θz ne renferme pas de terme indépendant, en sorte que la dernière condition exigée se trouve satisfaite d'elle-même.

Supposons maintenant que b ne soit pas nul suivant le module 7. La première des conditions écrites plus haut nous donne

$$c \equiv 3a^2 \pmod{7},$$

et, en substituant cette valeur, les deux autres se réduisent à

$$\left.\begin{array}{r} 3 - 3a^3 + b^2 \equiv 0 \\ a + a^4 \equiv 0 \end{array}\right\} \pmod{7};$$

il suit de là qu'on a ces deux solutions

$$\left.\begin{array}{ll} a \equiv 0, & b \equiv \pm 2 \\ a^3 \equiv -1, & b \equiv \pm 1 \end{array}\right\} \pmod{7}.$$

et

On conclut de là ces nouvelles formes réduites

$$\left.\begin{array}{l} \theta z \equiv z^5 \pm 2z^2 \\ \theta z \equiv z^5 + az^3 \pm z^2 + 3a^2 z \end{array}\right\} \pmod{7},$$

a étant ici un non-résidu quadratique de 7; enfin, par la transformation déjà employée plus haut, on ramènera ces deux formes aux suivantes :

$$\left.\begin{array}{l} \theta z \equiv z^5 + 2z^2 \\ \theta z \equiv z^5 + 3z^3 \pm z^2 - z \end{array}\right\} \pmod{7}.$$

En résumé, toutes les substitutions des indices

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,$$

au nombre de

$$1.2.3.4.5.6.7 = 5040,$$

peuvent être représentées par

$$\alpha z + \beta, \quad \alpha\theta(z + \beta) + \gamma,$$

la fonction θz prenant successivement ces formes :

$z^4 \pm 3z$,

$z^5 \pm 2z^2$,

$z^5 + az^3 + 3a^2 z$ (*a* quelconque),

$z^5 + az^3 \pm z^2 + 3a^2 z$ (*a* non résidu de 7).

487. M. Hermite a publié d'abord les résultats qui précèdent dans les *Annales* de M. Tortolini, et il les a complétés ensuite par des remarques que nous croyons utile de reproduire.

Considérons les deux formes réduites z^4+3z, z^5+2z^2, qui font partie de celles que nous avons obtenues, et distinguons les valeurs de z en deux groupes, contenant l'un les résidus quadratiques, l'autre les non-résidus, relativement au module 7. On trouvera

$$\begin{aligned} z^4+3z &\equiv 2z \quad (z \text{ résidu quadratique de } 7),\\ &\equiv 4z \quad (z \text{ non-résidu de } 7), \end{aligned}$$

et

$$\begin{aligned} z^5+2z^2 &\equiv 3z^2 \quad (z \text{ résidu quadratique de } 7),\\ &\equiv z^2 \quad (z \text{ non-résidu de } 7). \end{aligned}$$

Considérons en deuxième lieu la forme réduite z^5+z^3+3z, et distinguons les indices en résidus cubiques et en non-résidus relativement à 7; on aura

$$\begin{aligned} z^5+z^3+3z &\equiv -2z \quad (z \text{ résidu cubique de } 7),\\ &\equiv +2z \quad (z \text{ non-résidu cubique de } 7). \end{aligned}$$

Considérons enfin les deux substitutions z^5+3z^3-z et $z^5+3z^3\pm z^2-z$. On pourra encore ramener ces substitutions à la forme monôme, mais d'une manière toute différente. On a, en effet,

$$\begin{aligned} z^5+3z^3-z &\equiv 3z^2 \quad \left(z<\frac{7}{2}\right),\\ &\equiv -3z^2 \quad \left(z>\frac{7}{2}\right), \end{aligned}$$

d'où l'on conclut, en faisant $\varepsilon=\pm 1$,

$$\begin{aligned} z^5+3z^3+\varepsilon z^2-z &\equiv (3+\varepsilon)z^2 \quad \left(z<\frac{7}{2}\right),\\ &\equiv (-3+\varepsilon)z^2 \quad \left(z>\frac{7}{2}\right). \end{aligned}$$

Ces résultats, dit M. Hermite, autorisent jusqu'à un certain point à supposer que, dans l'étude des formes analytiques des substitutions pour un nombre premier p de lettres, les expressions nommées réduites se ramènent elles-mêmes à d'autres beaucoup plus simples, en considérant les valeurs de l'indice comme résidus ou non-résidus de puissances dont l'exposant diviserait $p-1$, ou bien encore comme divisées en deux séries formées l'une de nombres inférieurs à $\frac{p}{2}$, et l'autre de nombres supérieurs.

488. Par exemple, le nombre premier p étant quelconque, si l'on a une substitution réduite de la forme

$$\theta z = a z^{\omega}\left(z^{\frac{p-1}{2}}+1\right) - b z^{\varpi}\left(z^{\frac{p-1}{2}}-1\right),$$

il est clair que l'on peut écrire d'une manière plus simple

$$\theta z = 2az^{\omega} \quad (\text{si } z \text{ est résidu de } p),$$
$$\theta z = 2bz^{\varpi} \quad (\text{si } z \text{ est non-résidu de } p).$$

C'est à cette catégorie de substitutions qu'appartient, dans le cas de $p=7$, la substitution réduite

$$\theta z = -z^6 - 2z^3,$$

qui est telle, que l'on a

$$\theta[\theta z] = z$$

et

$$\theta[a\theta(z)+b] = 2ab^4\,\theta\left(z+\frac{2}{a^4 b}\right) + \frac{1-a}{a}(b^5+2b^2),$$

pourvu que a soit un résidu quadratique de 7.

Il résulte de là que, a étant résidu de 7, les substitutions représentées par les expressions

$$az+b,\quad a\theta(z+b)+c$$

forment un système conjugué. La première expression donne 3×3 ou 21 substitutions, la seconde en donne 3×7^2 ou 147. Donc il existe un système de 168 substitutions conjuguées de sept lettres; l'indice de ce système est égal à 80. Cet important résultat a été constaté pour la première fois par M. Kronecker.

CHAPITRE V.

APPLICATIONS DE LA THÉORIE DES SUBSTITUTIONS.

Des valeurs diverses que prend une fonction de plusieurs variables par les substitutions de ces variables.

489. Je me propose ici d'appliquer les principes établis dans les Chapitres précédents à l'étude des fonctions de plusieurs variables, au point de vue des valeurs diverses que prennent ces fonctions par les substitutions des variables.

Il suffit pour notre objet de considérer les fonctions rationnelles et même les fonctions entières; mais les développements qui vont suivre s'appliquent à toutes les fonctions *bien déterminées*.

Désignons par V une fonction bien déterminée des n variables

$$x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1};$$

formons les $N = 1.2.3\ldots n$ substitutions de ces variables, et exécutons successivement toutes ces substitutions dans la fonction V ; nous obtiendrons ainsi N résultats

$$(1)\qquad V,\ V^{(1)},\ V^{(2)},\ \ldots,\ V^{(N-1)}.$$

Si la fonction V est symétrique, les N résultats (1) seront tous égaux entre eux; au contraire, ils seront tous distincts si la fonction V n'offre aucune symétrie. Ce dernier cas se présentera en particulier si l'on a

$$V = \alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_{n-1} x_{n-1},$$

$\alpha_0,\ \alpha_1,\ \ldots,\ \alpha_{n-1}$ étant n coefficients inégaux.

Désignons généralement par μ le nombre de celles des fonctions (1) qui sont égales à V; alors μ sera le nombre des substitutions que l'on peut exécuter sur V sans changer cette fonction. Soient

$$(2) \qquad 1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1}$$

ces μ substitutions. Comme la fonction V ne change pas quand on exécute, dans un ordre quelconque, deux ou un plus grand nombre des substitutions (2), il est évident que ces substitutions constitueront un système conjugué.

Nous avons vu (n° 425) que les N substitutions des n variables peuvent être représentées par

$$(3) \qquad \begin{cases} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ T_1, & T_1S_1 & T_1S_2, & \ldots, & T_1S_{\mu-1}, \\ T_2, & T_2S_1 & T_2S_2, & \ldots, & T_2S_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T_{\nu-1}, & T_{\nu-1}S_1, & T_{\nu-1}S_2, & \ldots, & T_{\nu-1}S_{\mu-1}; \end{cases}$$

donc les $N = \mu\nu$ fonctions (1) pourront être représentées par

$$(4) \qquad \begin{cases} V_0, & V_0^{(1)}, & V_0^{(2)}, & \ldots, & V_0^{(\mu-1)}, \\ V_1, & V_1^{(1)}, & V_1^{(2)}, & \ldots, & V_1^{(\mu-1)}, \\ V_2, & V_2^{(1)}, & V_2^{(2)}, & \ldots, & V_2^{(\mu-1)}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ V_{\nu-1}, & V_{\nu-1}^{(1)}, & V_{\nu-1}^{(2)}, & \ldots, & V_{\nu-1}^{(\mu-1)}, \end{cases}$$

V_i^j désignant généralement le résultat obtenu en exécutant sur V, d'abord la substitution S_j, puis la substitution T_i; dans le cas de $j = 0$, la substitution S_j doit être réduite à l'unité, et nous écrivons V_i au lieu de V_i^0.

Comme les substitutions S ne changent pas V ou V_0, on voit que, dans le tableau (4), les termes d'une même ligne

horizontale sont égaux entre eux, et que les seules valeurs distinctes de V sont

$$(5) \qquad V_0, V_1, V_2, \ldots, V_{\nu-1}.$$

490. Lorsqu'une fonction ne sera pas altérée par une substitution, je dirai, pour abréger le discours, que la fonction *admet* la substitution ; on peut alors énoncer la proposition suivante :

THÉORÈME I. — *Les substitutions d'une fonction de plusieurs variables forment un système conjugué, et l'indice de ce système est égal au nombre des valeurs distinctes que la fonction peut acquérir par les substitutions.*

Ce théorème entraîne diverses conséquences (nos 426 et 444), parmi lesquelles nous devons signaler les suivantes :

COROLLAIRE I. — *Le nombre des valeurs distinctes d'une fonction de n variables est un diviseur du produit* $1.2.3\ldots n$.

COROLLAIRE II. — *Le nombre des valeurs distinctes d'une fonction de n variables ne peut s'abaisser au-dessous de n sans se réduire à* 1 *ou à* 2, *le cas de* $n = 4$ *étant seul excepté.*

COROLLAIRE III. — *Une fonction de n variables, qui a précisément n valeurs distinctes, est symétrique par rapport à* $n - 1$ *variables, le cas de* $n = 6$ *étant seul excepté.*

Il faut remarquer que, si l'on exécute une substitution quelconque sur les ν fonctions (5), ces fonctions ne pourront que s'échanger les unes dans les autres. Si donc on désigne par V une indéterminée, le produit

$$(V - V_0)(V - V_1)\ldots(V - V_{\nu-1})$$

sera une fonction symétrique. Il en résulte que toute fonction symétrique des fonctions (5) est une fonction symétrique des variables x; nous avons déjà eu l'occasion de faire cette remarque au n° 180.

491. La proposition que nous venons d'établir admet une réciproque que l'on peut énoncer comme il suit:

THÉORÈME II. — *Il existe toujours des fonctions qui admettent les substitutions d'un système conjugué donné et qui n'admettent aucune autre substitution.*

En effet, soient

$$(1) \qquad 1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1}$$

les substitutions conjuguées données, et désignons par X une fonction de n variables

$$x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1}$$

dont toutes les N valeurs soient distinctes; on pourra prendre, par exemple,

$$X = \alpha_0 x_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_{n-1} x_{n-1},$$

$\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ étant des nombres inégaux.

Soient

$$X_0,\ X_1,\ X_2,\ \ldots,\ X_{\mu-1}$$

les résultats obtenus en exécutant sur X les μ substitutions (1), et posons

$$V = X_0 X_1 X_2 \ldots X_{\mu-1},$$

il est évident que la fonction V admet les μ substitutions (1) et qu'elle n'admet aucune autre substitution.

REMARQUE. — Si l'on pose

$$V = f(X_0,\ X_1,\ X_2,\ \ldots,\ X_{\mu-1})$$

f désignant une fonction symétrique de $X_0, X_1, \ldots, X_{\mu-1}$, la fonction V admettra les substitutions (1); mais elle peut aussi en admettre d'autres, si la fonction f a une forme convenable. Si l'on fait, par exemple,

$$V = X_0 + X_1 + \ldots + X_{\mu-1},$$

V sera une fonction symétrique des variables $x_0, x_1, \ldots, x_{n-1}$.

Des fonctions semblables.

492. Deux fonctions de n variables sont dites ***semblables*** lorsqu'elles admettent les mêmes substitutions.

Ainsi les fonctions

$$x_0x_1 + x_2x_3, \quad (x_0 + x_1)(x_2 + x_3)$$

des quatre variables x_0, x_1, x_2, x_3 sont semblables, car elles admettent les huit mêmes substitutions :

$$1 \left| \begin{matrix} (x_0, x_1) \\ (x_2, x_3) \end{matrix} \right| \begin{matrix} (x_0, x_2)(x_1, x_3) \\ (x_0, x_3)(x_1, x_2) \end{matrix} \left| \begin{matrix} (x_0, x_2, x_1, x_3) \\ (x_0, x_1)(x_2, x_3) \\ (x_0, x_3, x_1, x_2) \end{matrix} \right|,$$

qui forment un système conjugué dont l'indice est égal à 3.

Lagrange a fait connaître une propriété importante des fonctions semblables que l'on peut énoncer ainsi :

Étant données deux fonctions semblables des n variables $x_0, x_1, x_2, \ldots, x_{n-1}$, chacune de ces fonctions est exprimable par une fonction rationnelle de l'autre, dans laquelle les coefficients sont des fonctions symétriques des n variables.

Cette proposition est contenue dans une autre plus générale que nous allons établir :

THÉORÈME. — *Étant données deux fonctions des*

n variables $x_0, x_1, \ldots, x_{n-1}$, savoir :

$$V = F(x_0, x_1, x_2, \ldots, x_{n-1}),$$
$$y = f(x_0, x_1, x_2, \ldots, x_{n-1}),$$

si la fonction y admet toutes les substitutions de la fonction V, elle est exprimable par une fonction rationnelle de V, dans laquelle les coefficients sont des fonctions symétriques.

En effet, soient

$$1, S_1, S_2, \ldots, S_{\mu-1}$$

les substitutions conjuguées de V, et

$$1, T_1, T_2, \ldots, T_{\nu-1}$$

les ν substitutions par lesquelles on déduit respectivement de V les ν valeurs distinctes que cette fonction peut acquérir ; supposons enfin que V_ρ et y_ρ soient les résultats obtenus en exécutant la substitution T_ρ sur V et sur y. Nous regardons T_0 comme égale à 1, et, en conséquence, V_0 et y_0 ne seront autre chose que V et y.

Si l'on fait

$$\psi(V) = (V - V_0)(V - V_1)(V - V_2)\ldots(V - V_{\nu-1}),$$

on aura, en développant,

$$\psi(V) = V^\nu + P_1 V^{\nu-1} + P_2 V^{\nu-2} + \ldots + P_{\nu-1} V + P_\nu,$$

$P_1, P_2, \ldots, P_\nu$ étant des fonctions symétriques. Ici V est regardée comme une indéterminée, et l'équation

(1) $$\psi(V) = 0$$

a pour racines

(2) $$V_0, V_1, V_2, \ldots, V_{\nu-1}.$$

Considérons maintenant la fonction

$$V^m y,$$

où m est un nombre entier quelconque ; par hypothèse, cette fonction admet toutes les substitutions de V ; si elle en admet un plus grand nombre, ces substitutions pourront être représentées par

$$\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ R_1, & R_1 S_1, & R_1 S_2, & \ldots, & R_1 S_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ R_{\rho-1}, & R_{\rho-1} S_1, & R_{\rho-1} S_2, & \ldots, & R_{\rho-1} S_{\mu-1}, \end{array}$$

et, en multipliant par certaines substitutions

$$1, Q_1, Q_2, \ldots, Q_{\lambda-1},$$

on formera (n° 425) toutes les $1.2.3\ldots n$ substitutions des n variables. Il résulte de là que les substitutions T sont les produits des substitutions

$$1, R_1, R_2, \ldots, R_{\rho-1},$$

qui ne changent pas $V^m y$, par les substitutions

$$1, Q_1, Q_2, \ldots, Q_{\lambda-1}.$$

Ainsi, en appliquant à la fonction $V^m y$ les ν substitutions T, on obtiendra les λ valeurs distinctes de cette fonction, répétées chacune ρ fois; par conséquent la somme

$$V_0^m y_0 + V_1^m y_1 + V_2^m y_2 + \ldots + V_{\nu-1}^m y_{\nu-1}$$

est une fonction symétrique des n variables $x_0, x_1, \ldots,$

x_{n-1}. Si donc on donne à m les valeurs successives 0, 1, 2, ..., $(\nu-1)$, et que l'on pose

$$(3)\quad \begin{cases} y_0 + y_1 + y_2 + \ldots + y_{\nu-1} = t_0, \\ V_0 y_0 + V_1 y_1 + V_2 y_2 + \ldots + V_{\nu-1} y_{\nu-1} = t_1, \\ V_0^2 y_0 + V_1^2 y_1 + V_2^2 y_2 + \ldots + V_{\nu-1}^2 y_{\nu-1} = t_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ V_0^{\nu-1} y_0 + V_1^{\nu-1} y_1 + \ldots\ldots + V_{\nu-1}^{\nu-1} y_{\nu-1} = t_{\nu-1}, \end{cases}$$

t_0, t_1, ... seront des fonctions symétriques.

Ajoutons les équations (3), après les avoir multipliées respectivement par les facteurs indéterminés

$$\lambda_0,\ \lambda_1,\ \lambda_2,\ \ldots,\ \lambda_{\nu-2},\ 1,$$

et faisons, pour abréger,

$$(4)\quad \varphi(V) = V^{\nu-1} + \lambda_{\nu-2} V^{\nu-2} + \ldots + \lambda_1 V + \lambda_0,$$

on aura

$$(5)\quad \begin{cases} y_0 \varphi(V_0) + y_1 \varphi(V_1) + \ldots + y_{\nu-1} \varphi(V_{\nu-1}) \\ \quad = t_0 \lambda_0 + t_1 \lambda_1 + \ldots + t_{\nu-2} \lambda_{\nu-2} + t_{\nu-1}, \end{cases}$$

et si l'on veut la valeur de y_ρ par exemple, il suffira de déterminer les facteurs λ_0, λ_1, ..., de manière que l'on ait

$$(6)\quad \varphi(V_0) = 0, \quad \varphi(V_1) = 0, \quad \ldots, \quad \varphi(V_{\nu-1}) = 0,$$

excepté $\varphi(V_\rho) = 0$; alors l'équation (5) donnera

$$(7)\quad y_\rho = \frac{t_0 \lambda_0 + t_1 \lambda_1 + \ldots + t_{\nu-2} \lambda_{\nu-2} + t_{\nu-1}}{\varphi(V_\rho)},$$

et il ne restera plus qu'à trouver les valeurs de λ_0, λ_1, ..., ce que l'on peut faire très-aisément de la manière suivante.

Les équations (6) qui déterminent ces facteurs expriment que l'équation

$$\varphi(V) = 0$$

a pour racines $V_0, V_1, \ldots, V_{\nu-1}$, excepté V_ρ; mais l'équation (1)

$$\psi(V) = 0$$

a ces mêmes racines, y compris V_ρ; et comme, d'ailleurs, les plus hautes puissances de V dans $\varphi(V)$ et dans $\psi(V)$ ont pour coefficient l'unité, on aura identiquement

$$\varphi(V) = \frac{\psi(V)}{V - V_\rho},$$

ou, en développant le quotient de $\psi(V)$ par $V - V_\rho$,

$$\varphi(V) = V^{\nu-1} + \left.\begin{matrix} P_1 \\ + V_\rho \end{matrix}\right| V^{\nu-2} + \left.\begin{matrix} P_2 \\ + P_1 V_\rho \\ + V_\rho^2 \end{matrix}\right| V^{\nu-3} + \ldots + \begin{matrix} P_{\nu-1} \\ + P_{\nu-2} V_\rho \\ + P_{\nu-3} V_\rho^2 \\ \cdots\cdots \\ + P_1 V_\rho^{\nu-2} \\ + V_\rho^{\nu-1}. \end{matrix}$$

En identifiant cette valeur de $\varphi(V)$ avec celle donnée par l'équation (4), on obtient les valeurs suivantes des facteurs λ :

$$(8)\quad \left\{\begin{array}{l} \lambda_{\nu-2} = P_1 + V_\rho, \\ \lambda_{\nu-3} = P_2 + P_1 V_\rho + V_\rho^2, \\ \lambda_{\nu-4} = P_3 + P_2 V_\rho + P_1 V_\rho^2 + V_\rho^3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \lambda_0 \ldots = P_{\nu-1} + P_{\nu-2} V_\rho + \ldots + P_1 V_\rho^{\nu-2} + V_\rho^{\nu-1}. \end{array}\right.$$

Ces facteurs étant tous exprimés en fonction de V_ρ et des fonctions symétriques, il en sera de même de y_ρ. On peut

donner à l'expression de y_ρ une forme très-simple ; si l'on fait, pour abréger l'écriture,

$$\begin{aligned}
s_{\nu-1} &= t_{\nu-1} + P_1 t_{\nu-2} + P_2 t_{\nu-3} + \ldots + P_{\nu-2} t_1 + P_{\nu-1} t_0,\\
s_{\nu-2} &= t_{\nu-2} + P_1 t_{\nu-3} + P_2 t_{\nu-4} + \ldots + P_{\nu-2} t_0,\\
s_{\nu-3} &= t_{\nu-3} + P_1 t_{\nu-4} + \ldots + P_{\nu-3} t_0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
s_1 &= t_1 + P_1 t_0,\\
s_0 &= t_0,
\end{aligned}$$

et que l'on désigne par $\Theta(V_\rho)$ le numérateur de la valeur de y_ρ, donnée par l'équation (7), on aura

$$(9) \qquad \Theta(V_\rho) = s_0 V_\rho^{\nu-1} + s_1 V_\rho^{\nu-2} + \ldots + s_{\nu-2} V_\rho + s_{\nu-1}.$$

Quant au dénominateur de l'expression de y_ρ, il est égal à $\varphi(V_\rho)$, c'est-à-dire à la valeur que prend la fraction $\dfrac{\psi(V)}{V - V_\rho}$ pour $V = V_\rho$: cette valeur est

$$(10) \qquad \psi'(V_\rho) = \nu V_\rho^{\nu-1} + (\nu - 1) P_1 V_\rho^{\nu-2} + \ldots + P_{\nu-1},$$

ψ' désignant la dérivée de ψ. On a donc

$$(11) \qquad y_\rho = \frac{\Theta(V_\rho)}{\psi'(V_\rho)}$$

ou

$$(12) \qquad y = \frac{\Theta(V)}{\psi'(V)},$$

en désignant simplement par V l'une quelconque des valeurs V_0, V_1, ... et par y la valeur correspondante de la suite y_0, y_1, ...

La formule précédente démontre le théorème énoncé, et elle donne l'expression de y en fonction rationnelle de V. Ajoutons que, par la méthode exposée au n° 182,

on pourra donner à la formule (12) la forme plus simple

$$y = \Pi(V),$$

$\Pi(V)$ désignant une fonction entière du degré $\nu - 1$ au plus, dans laquelle les coefficients de V sont des fonctions symétriques des variables x.

Sur la formation des fonctions de n variables, qui admettent des substitutions données.

493. Le problème qui a pour objet de former les fonctions de n variables, dont le nombre des valeurs distinctes est égal à un nombre donné ν, se ramène, d'après les théorèmes précédents, à la détermination des systèmes de substitutions conjuguées dont l'indice est égal à ν. Effectivement, quand on connaîtra un tel système, on obtiendra sans difficulté, par le théorème du n° 491, une fonction particulière V correspondante, qui aura précisément ν valeurs distinctes. Et, quant aux autres fonctions semblables, elles seront toutes exprimables, comme on vient de le voir, par des fonctions entières de V du degré $\nu - 1$, dans lesquelles les coefficients des puissances de V seront des fonctions symétriques.

Considérons, par exemple, les fonctions qui ont deux valeurs distinctes. Les substitutions de ces fonctions forment un système conjugué dont l'indice est égal à 2; ce système est unique, comme on l'a vu au n° 429, et il se compose des substitutions qui équivalent à un nombre pair de transpositions. Les fonctions V dont nous nous occupons sont donc semblables, et si l'on désigne par P l'une d'elles, l'expression générale de V sera

$$V = A + BP,$$

A et B étant des fonctions symétriques. On peut prendre

pour P la fonction alternée des n variables $x_0, x_1, \ldots, x_{n-1}$, dont nous nous sommes occupés au n° 236 et qui a pour expression

$$P = (x_1 - x_0)(x_2 - x_0)\ldots(x_{n-1} - x_0)(x_2 - x_1)\ldots(x_{n-1} - x_{n-2}).$$

Il est évident que les fonctions qui ont deux valeurs distinctes admettent toutes les substitutions circulaires du troisième ordre qu'on peut former avec les variables, et qu'elles n'admettent aucune transposition.

Parmi les fonctions qui répondent à un système donné de substitutions conjuguées, on peut se proposer de déterminer les plus simples, par exemple celles qui, étant rationnelles et entières, ont le plus petit degré. Énoncé dans ces termes, le problème qui nous occupe exige des considérations d'un tout autre ordre, et sa solution offre de sérieuses difficultés. Nous n'aborderons point ici l'étude de ce nouveau problème, qui est d'ailleurs tout à fait en dehors de notre sujet ; toutefois, afin de présenter une application de la théorie que nous avons développée dans les Chapitres précédents, nous croyons utile de faire connaître ici un procédé particulier par lequel on obtient facilement les fonctions qui répondent à certains systèmes de substitutions conjuguées.

Si un système de substitutions conjuguées est m fois transitif, nous dirons, avec Cauchy, que les fonctions qui admettent ces substitutions sont m fois *transitives*.

Des fonctions doublement transitives de n variables qui ont $1.2.3\ldots(n-2)$ valeurs, n étant premier.

494. Les fonctions dont il s'agit ici jouent un rôle considérable dans la théorie des équations algébriques. Elles répondent au système conjugué formé par les

$n(n-1)$ substitutions linéaires et entières de la forme

$$\begin{pmatrix} az+b \\ z \end{pmatrix},$$

z désignant successivement tous les indices 0, 1, 2, ..., $(n-1)$ des n variables

$$(1) \qquad x_0, \; x_1, \; x_2, \; \ldots, \; x_{n-1},$$

et les valeurs de $az+b$ étant prises, suivant le module n, entre les limites zéro et $n-1$.

Soit α une racine de l'équation

$$(2) \qquad \frac{x^n-1}{x-1}=0,$$

et posons

$$(3) \qquad t=x_0+\alpha x_1+\alpha^2 x_2+\ldots+\alpha^{n-1}x_{n-1}:$$

il est évident que t est une fonction des n variables (1) qui a $1.2.3\ldots n$ valeurs distinctes.

Exécutons, sur la fonction t, la substitution d'ordre n

$$\begin{pmatrix} z+1 \\ z \end{pmatrix},$$

ainsi que les puissances successives de cette substitution. On obtiendra n résultats

$$(4) \qquad t_0, \; t_1, \; t_2, \; \ldots, \; t_{n-1}$$

et comme t_μ se déduit de t en remplaçant chaque indice z par $z+\mu$, on aura

$$t_\mu = x_\mu + \alpha x_{\mu+1} + \ldots + \alpha^j x_{\mu+j} + \ldots + \alpha^{n-1} x_{\mu+n-1}.$$

Soit

$$\mu+j\equiv i \quad \text{ou} \quad j\equiv i-\mu \quad (\text{mod. } n),$$

i étant compris entre zéro et $n-1$, il viendra

$$t_\mu=\alpha^{-\mu}(x_0+\alpha x_1+\alpha^2 x_2+\ldots+\alpha^{n-1}x_{n-1})$$

ou

$$t_\mu=\alpha^{-\mu}t;$$

ainsi chacune des fonctions (4) est égale au produit de t par une puissance de α, et comme on a

$$\alpha^n = 1,$$

les fonctions dont il s'agit ont la même puissance $n^{\text{ième}}$. Si donc on pose $\theta = t^n$, ou

$$(5) \qquad \theta = (x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1})^n,$$

la fonction θ sera invariable par la substitution circulaire $\begin{pmatrix} z+1 \\ z \end{pmatrix}$, et il est évident que le nombre de ses valeurs distinctes sera

$$1.2.3\ldots(n-1).$$

Maintenant désignons par r une racine primitive pour le nombre premier n, et exécutons sur les indices z des variables x les puissances $0, 1, 2, \ldots, (n-2)$ de la substitution circulaire, d'ordre $n-1$,

$$\begin{pmatrix} rz \\ z \end{pmatrix};$$

on obtiendra ainsi $n-1$ résultats que nous représenterons par

$$(6) \qquad \theta_0,\ \theta_1,\ \theta_2,\ \ldots,\ \theta_{n-2}.$$

On aura généralement

$$\theta_\mu = (x_0 + \alpha x_{r^\mu} + \ldots + \alpha^j x_{jr^\mu} + \ldots)^n,$$

et si l'on pose

$$jr^\mu \equiv i, \quad j \equiv ir^{n-1-\mu} \pmod{n},$$

i étant compris entre zéro et $n-1$, il viendra

$$\theta_\mu = (x_0 + \ldots + \alpha^{ir^{n-1-\mu}} x_i + \ldots)^n,$$

d'où il suit que θ_μ se déduit de θ en remplaçant α par

$^{-1-\mu}$. Or, si l'on donne à μ les valeurs successives

$$0,\ 1,\ 2,\ \ldots,\ (n-2),$$

$^{-1-\mu}$ prendra toutes les valeurs

$$1,\ 2,\ 3,\ \ldots,\ n-1)$$

vant le module n, et, par conséquent, l'expression $^{-1-\mu}$ donnera successivement les $n-1$ racines

$$\alpha,\ \beta,\ \gamma,\ \ldots,\ \omega$$

l'équation (2). Donc les valeurs des fonctions (6) s'obndront en remplaçant α par chacune des racines (7) ns l'expression de θ; on a ainsi

$$\left\{\begin{array}{l} \theta_0 = (x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1})^n, \\ \theta_1 = (x_0 + \beta x_1 + \beta^2 x_2 + \ldots + \beta^{n-1} x_{n-1})^n, \\ \theta_2 = (x_0 + \gamma x_1 + \gamma^2 x_2 + \ldots + \gamma^{n-1} x_{n-1})^n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \theta_{n-2} = (x_0 + \omega x_1 + \omega^2 x_2 + \ldots + \omega^{n-1} x_{n-1})^n. \end{array}\right.$$

hacune des fonctions (8) est invariable par la substin $\begin{pmatrix} z+1 \\ z \end{pmatrix}$, et quand on applique à ces fonctions la titution $\begin{pmatrix} rz \\ z \end{pmatrix}$, elles se changent les unes dans les es ; si donc on désigne par θ une indéterminée, la tion

$$(\theta-\theta_0)(\theta-\theta_1)(\theta-\theta_2)\ldots(\theta-\theta_{n-2})$$

nettra les substitutions

$$\begin{pmatrix} z+1 \\ z \end{pmatrix},\quad \begin{pmatrix} rz \\ z \end{pmatrix};$$

ar suite, elle admettra toutes les substitutions linéaires

et entières

$$\begin{pmatrix} \lambda z \\ z \end{pmatrix},$$

et le nombre de ses valeurs distinctes sera $1.2.3\ldots(n-2)$.

Il est évident que toutes les fonctions symétriques de θ_0, $\theta_1, \ldots, \theta_{n-2}$ admettent les substitutions linéaires et entières; ces fonctions sont donc deux fois transitives.

495. Si d désigne un diviseur de $n-1$, que l'on fasse

$$n-1 = de,$$

et qu'on applique à la fonction θ les puissances de la substitution régulière

$$\begin{pmatrix} r^d z \\ z \end{pmatrix},$$

qui est de l'ordre e, on obtiendra e résultats

$$\theta_0, \theta_1, \theta_2, \ldots, \theta_{e-1},$$

et il est évident que la fonction

$$(\theta-\theta_0)(\theta-\theta_1)\ldots(\theta-\theta_{e-1})$$

aura $1.2.3\ldots(n-2)\times d$ valeurs distinctes.

Des fonctions triplement transitives de n + 1 variables qui ont 1.2.3...(n — 2) valeurs, n étant premier.

496. L'existence des fonctions dont il s'agit est évidente *à priori*; ces fonctions répondent au système conjugué formé par les $(n+1)n(n-1)$ substitutions linéaires relatives au module premier n. La règle que je vais exposer pour les obtenir ne diffère que dans la forme de celle qui a été donnée pour la première fois par M. Émile Mathieu.

Le nombre n étant supposé premier, considérons d'abord les n variables

(1) $$x_0, x_1, x_2, \ldots, x_{n-1},$$

et posons, comme au n° 494,

$$(2)\quad \left\{\begin{array}{l} \theta_0 = (x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1})^n, \\ \theta_1 = (x_0 + \beta x_1 + \beta^2 x_2 + \ldots + \beta^{n-1} x_{n-1})^n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \theta_{n-2} = (x_0 + \omega x_1 + \omega^2 x_2 + \ldots + \omega^{n-1} x_{n-1})^n, \end{array}\right.$$

$\alpha, \beta, \gamma, \ldots, \omega$ étant les $n-1$ racines de l'équation

$$\frac{x^n - 1}{x - 1} = 0.$$

Soit ν une fonction rationnelle et symétrique quelconque des $n-1$ expressions (2) : cette fonction ν sera invariable, comme nous l'avons vu, par toute substitution de la forme

$$(3)\qquad \begin{pmatrix} \lambda z \\ z \end{pmatrix},$$

λz étant une fonction entière quelconque de l'indice z.

D'après la théorie des fonctions semblables, toute fonction des variables (1) qui admet les substitutions (3) est une fonction rationnelle de ν dans laquelle les coefficients des puissances de ν sont des fonctions symétriques. Désignons donc par V_0 une fonction rationnelle arbitraire de la quantité ν et d'une nouvelle variable que je représenterai par x_∞ ; V_0 sera une fonction des $n+1$ variables

$$x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1},\ x_\infty,$$

qui sera invariable par toutes les substitutions entières et linéaires ; on peut, si l'on veut, prendre pour V_0 la fonction ν elle-même.

Cela posé, soit θz une *fonction rationnelle linéaire* d'ordre $n+1$ pour le module n, et désignons par V_i la valeur que prend V_0 quand on exécute i fois sur cette fonction la substitution

$$\begin{pmatrix} \theta z \\ z \end{pmatrix},$$

ce que l'on peut exprimer en écrivant, d'après la notation de Cauchy,

$$(4) \qquad V_i = \begin{pmatrix} \theta^i z \\ z \end{pmatrix} V_0.$$

Soit encore ϖz une fonction rationnelle linéaire d'ordre quelconque pour le module n, et exécutons sur V_i la substitution

$$\begin{pmatrix} \varpi z \\ z \end{pmatrix};$$

on obtiendra un résultat qui peut être représenté par

$$\begin{pmatrix} \varpi z \\ z \end{pmatrix} V_i = \begin{pmatrix} \varpi\theta^i z \\ z \end{pmatrix} V_0.$$

Or, si j désigne un entier quelconque, comme la fonction θz est d'ordre $n+1$, on pourra effectuer la substitution $\begin{pmatrix} \varpi\theta^i z \\ z \end{pmatrix}$ en faisant d'abord la substitution $\begin{pmatrix} \theta^j\varpi\theta^i z \\ z \end{pmatrix}$, puis la substitution $\begin{pmatrix} \theta^{n+1-j} z \\ z \end{pmatrix}$. On peut donc écrire

$$\begin{pmatrix} \varpi z \\ z \end{pmatrix} V_i = \begin{pmatrix} \theta^{n+1-j} z \\ z \end{pmatrix} \begin{pmatrix} \theta^j\varpi\theta^i z \\ z \end{pmatrix} V_0,$$

égalité où chacun des nombres i et j est arbitraire. Mais, d'après le théorème du n° 484, à chaque valeur de l'un des nombres i, j correspond pour l'autre nombre une valeur telle, que

$$\begin{pmatrix} \theta^j\varpi\theta^i z \\ z \end{pmatrix}$$

est une substitution entière; et en outre, quand l'un des nombres i, j reçoit successivement les $n+1$ valeurs $0, 1, 2, \ldots, n$, l'autre nombre prend aussi toutes ces mêmes valeurs. Si donc i et j sont choisis de manière à réaliser les conditions du théorème que je viens de

rappeler, comme V_0 est invariable par les substitutions linéaires et entières, on aura

$$\binom{\varpi z}{z} V_i = \binom{\theta^{n+1-j} z}{z} V_0,$$

ou, d'après la formule (4),

$$(5) \qquad \binom{\varpi z}{z} V_i = V_{n+1-j},$$

et, je le répète, si dans cette formule l'un des nombres i, j prend successivement les $n+1$ valeurs $0, 1, 2, \ldots, n$, l'autre nombre prendra aussi successivement toutes ces mêmes valeurs.

La formule (5) exprime cette conséquence remarquable, que *les* $n+1$ *fonctions*

$$(6) \qquad V_0, V_1, V_2, \ldots, V_n$$

forment un système qui est invariable par une substitution linéaire quelconque, c'est-à-dire qu'une telle substitution ne peut qu'échanger entre elles les fonctions du système.

Si donc T désigne une fonction symétrique des expressions (6), que l'on fasse, par exemple,

$$(7) \qquad T = (V - V_0)(V - V_1) \ldots (V - V_n),$$

V étant une indéterminée, la fonction T admettra toutes les substitutions linéaires; elle sera donc triplement transitive, et elle aura $1.2.3\ldots(n-2)$ valeurs distinctes.

Si l'on désigne par T_1 et T_2 deux fonctions semblables à la fonction T, par P la fonction alternée

$$(x_1 - x_0) \ldots (x_1 - x_\infty)(x_2 - x_1) \ldots (x_\infty - x_{n-1})$$

des $n+1$ variables, et que l'on fasse

$$S = T_1 + PT_2,$$

la fonction S admettra toutes les substitutions linéaires dont le déterminant est résidu quadratique de n, et qui équivalent en conséquence à un nombre pair de transpositions. S aura donc $2 \times 1.2\ldots(n-2)$ valeurs distinctes, ainsi que M. Mathieu en a fait la remarque. On peut aussi former les fonctions S de la même manière que les fonctions T, en faisant usage du corollaire du nº 484; mais nous devons nous borner à cette indication.

Sur les fonctions triplement transitives de six variables qui ont six valeurs distinctes.

497. On peut donner plusieurs formes diverses aux fonctions dont nous venons de nous occuper; nous prendrons comme exemple le cas des fonctions transitives de six lettres qui ont six valeurs distinctes.

Les variables étant désignées par

$$x_0,\ x_1,\ x_2,\ x_3,\ x_4,\ x_\infty,$$

nous poserons

$$V_0 = x_\infty x_0 + x_1 x_4 + x_2 x_3,$$

et, les indices z étant pris suivant le module 5, nous effectuerons sur V_0 la substitution du cinquième ordre

$$\begin{pmatrix} z+1 \\ z \end{pmatrix} = (0,\ 1,\ 2,\ 3,\ 4)$$

et ses puissances; on trouve alors les résultats suivants:

$$\left\{\begin{aligned}
V_0 &= x_\infty x_0 + x_1 x_4 + x_2 x_3,\\
V_1 &= x_\infty x_1 + x_2 x_0 + x_3 x_4,\\
V_2 &= x_\infty x_2 + x_3 x_1 + x_4 x_0,\\
V_3 &= x_\infty x_3 + x_4 x_2 + x_0 x_1,\\
V_4 &= x_\infty x_4 + x_0 x_3 + x_1 x_2.
\end{aligned}\right.$$

Ensuite, si l'on fait

$$T = (V - V_0)(V - V_1)(V - V_2)(V - V_3)(V - V_4),$$

V étant une indéterminée, la fonction T sera invariable par toutes les substitutions linéaires et entières, et, comme elle n'est pas symétrique, elle aura précisément six valeurs distinctes. Pour justifier cette assertion, il suffit d'établir que la fonction T est invariable par deux substitutions linéaires, l'une du quatrième ordre, l'autre du sixième. La substitution du quatrième ordre

$$\binom{2z}{z} = (1,\ 2,\ 4,\ 3)$$

laisse V_0 invariable, et elle change

$$V_1,\ V_2,\ V_3,\ V_4$$

en

$$V_2,\ V_4,\ V_1,\ V_3;$$

ensuite la substitution du sixième ordre

$$\left(\begin{matrix}\left(\dfrac{z+3}{z}\right)\\ z\end{matrix}\right) = (0,\ \infty,\ 1,\ 4,\ 3,\ 2)$$

change

$$V_0,\ V_1,\ V_2,\ V_3,\ V_4$$

en

$$V_1,\ V_0,\ V_3,\ V_4,\ V_2,$$

ce qui achève la démonstration de notre proposition.

Méthode de Lagrange pour calculer une fonction des racines d'une équation donnée, quand on connaît une autre fonction quelconque des racines.

498. Parmi les travaux publiés depuis un siècle sur la théorie algébrique des équations, l'un des plus importants est, sans contredit, le célèbre Mémoire de Lagrange, que nous avons déjà eu l'occasion de citer (n° 189), et qui fait partie des *Mémoires de l'Académie de Berlin*

pour 1770 et 1771. On rencontre, entre autres résultats remarquables, dans ce grand travail, le beau théorème que voici :

Dès qu'on aura trouvé, par un moyen quelconque, la valeur d'une fonction rationnelle des racines d'une équation, on pourra, en général, trouver la valeur d'une autre fonction rationnelle quelconque des mêmes racines, et cela par le moyen d'une équation simplement linéaire. Quelques cas particuliers exigeront cependant la résolution d'une équation du deuxième, du troisième, etc., degré.

Soient

$$x_0,\ x_1,\ \ldots,\ x_{n-1}$$

les n racines de l'équation

$$(1)\qquad x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n = 0,$$

et

$$V = F(x_0,\ x_1,\ \ldots,\ x_{n-1}),$$
$$y = f(x_0,\ x_1,\ \ldots,\ x_{n-1})$$

deux fonctions rationnelles de ces racines dont la première a une valeur donnée.

Nous supposerons d'abord que la fonction f admette toutes les substitutions de F ; dans ce cas, on peut déterminer la valeur de f par la méthode dont nous avons fait usage au n° 492. Effectivement, si l'on représente par

$$(2)\qquad V_0,\ V_1,\ V_2,\ \ldots,\ V_{\nu-1}$$

les valeurs distinctes que prend F par les substitutions, et par

$$(3)\qquad y_0,\ y_1,\ y_2,\ \ldots,\ y_{\nu-1}$$

les valeurs correspondantes de f, que l'on pose en outre,

comme au n° 492,

$$(4)\quad \begin{cases} y_0+y_1+y_2+\ldots+y_{\nu-1}=t_0,\\ V_0y_0+V_1y_1+V_2y_2+\ldots+V_{\nu-1}y_{\nu-1}=t_1,\\ V_0^2y_0+V_1^2y_1+V_2^2y_2+\ldots+V_{\nu-1}^2y_{\nu-1}=t_2,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ V_0^{\nu-1}y_0+V_1^{\nu-1}y_1+V_2^{\nu-1}y_2+\ldots+V_{\nu-1}^{\nu-1}y_{\nu-1}=t_{\nu-1}, \end{cases}$$

on pourra exprimer $t_0, t_1, \ldots, t_{\nu-1}$ en fonction des quantités connues, puisque ce sont des fonctions symétriques des racines de l'équation (1). Ensuite la résolution des équations (4) fera connaître les inconnues $y_0, y_1, \ldots$.

Nous avons vu que, si l'on représente par

$$(5)\qquad \psi(V)=V^{\nu-1}+P_1V^{\nu-2}+\ldots+P_{\nu-1}V+P_\nu$$

le polynôme égal au produit

$$(V-V_0)(V-V_1)\ldots(V-V_{\nu-1}),$$

par $\psi'(V)$ la dérivée de V, puis que l'on fasse, pour abréger,

$$(6)\quad \begin{cases} s_{\nu-1}=t_{\nu-1}+P_1t_{\nu-2}+P_2t_{\nu-3}+\ldots+P_{\nu-2}t_1+P_{\nu-1}t_0,\\ s_{\nu-2}=t_{\nu-2}+P_1t_{\nu-3}+P_2t_{\nu-4}+\ldots+P_{\nu-2}t_0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ s_1=t_1+P_1t_0,\\ s_0=t_0 \end{cases}$$

et

$$(7)\qquad \Theta(V)=s_0V^{\nu-1}+s_1V^{\nu-2}+\ldots+s_{\nu-2}V+s_{\nu-1},$$

les valeurs des inconnues y sont

$$(8)\quad y_0=\frac{\Theta(V_0)}{\psi'(V_0)},\quad y_1=\frac{\Theta(V_1)}{\psi'(V_1)},\quad \ldots,\quad y_{\nu-1}=\frac{\Theta(V_{\nu-1})}{\psi'(V_{\nu-1})}.$$

Dans l'hypothèse où nous nous sommes placé, la fonc-

tion F a ν valeurs distinctes *algébriquement;* mais ici x_0, x_1, ..., x_{n-1} ne sont plus des indéterminées, et il peut arriver que plusieurs des quantités (2) soient *numériquement* égales entre elles. Lorsque ce cas se présente, l'équation

$$\psi(V) = 0 \tag{9}$$

a des racines multiples, et quelques-unes des formules (8) deviennent illusoires; mais, dans tous les cas, si V_ρ est une racine simple de l'équation (9), la formule

$$y_\rho = \frac{\Theta(V_\rho)}{\psi'(V_\rho)}$$

donnera toujours, comme nous allons le démontrer, la valeur de y qui répond à la valeur V_ρ de V.

499. On voit, d'après ce qui précède, qu'il est nécessaire de compléter l'analyse du n° 492 pour l'adapter au cas qui nous occupe ici. Supposons que, parmi les quantités (2), il y en ait i qui soient numériquement distinctes et représentons-les par

$$V_0,\ V_1,\ V_2,\ \ldots,\ V_{i-1}. \tag{10}$$

Soient V_ρ l'une des quantités (10) et Y_ρ la somme de toutes les valeurs de y qui répondent aux valeurs de V égales à V_ρ. Les équations (4) deviendront

$$(11)\quad \left\{ \begin{array}{r} Y_0 + Y_1 + \ldots + Y_{i-1} = t_0, \\ V_0 Y_0 + V_1 Y_1 + \ldots + V_{i-1} Y_{i-1} = t_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ V_0^{i-1} Y_0 + V_1^{i-1} Y_1 + \ldots + V_{i-1}^{i-1} Y_{i-1} = t_{i-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ V_0^{\nu-1} Y_0 + V_1^{\nu-1} Y_1 + \ldots + V_{i-1}^{\nu-1} Y_{i-1} = t_{\nu-1}; \end{array} \right.$$

il est évident qu'elles ne peuvent déterminer que les i quantités

$$Y_0, Y_1, \ldots, Y_{i-1},$$

et que les i premières équations suffisent en toute rigueur pour cet objet; mais nous en emploierons un plus grand nombre, afin d'arriver à des formules où ne figurent que les deux seules fonctions $\Theta(V)$, $\psi(V)$ déjà introduites.

Désignons par r le nombre des quantités (2) qui sont égales à V_ρ et considérons les $\nu - r + 1$ premières équations (11); dans le cas de $r = 1$, aucune équation ne sera exclue. Ajoutons les équations dont il s'agit, après les avoir multipliées par les facteurs

$$\theta_0, \theta_1, \ldots, \theta_{\nu-r-1}, 1,$$

et faisons, pour abréger,

$$(12) \qquad \varphi(V) = V^{\nu-r} + \theta_{\nu-r-1} V^{\nu-r-1} + \ldots + \theta_1 V + \theta_0,$$

on aura

$$Y_0 \varphi(V_0) + Y_1 \varphi(V_1) + \ldots + Y_{i-1} \varphi(V_{i-1})$$
$$= \theta_0 t_0 + \theta_1 t_1 + \ldots + \theta_{\nu-r-1} t_{\nu-r-1} + t_{\nu-r}.$$

et si l'on détermine les facteurs θ, de manière que l'on ait identiquement

$$\varphi(V) = \frac{\psi(V)}{(V - V_\rho)^r},$$

la précédente équation donnera

$$(13) \qquad Y_\rho = \frac{\theta_0 t_0 + \theta_1 t_1 + \ldots + \theta_{\nu-r-1} t_{\nu-r-1} + t_{\nu-r}}{\varphi(V_\rho)}.$$

L'expression de $\varphi(V)$ s'obtient facilement en multipliant les deux expressions

$$\psi(V) = V^\nu + P_1 V^{\nu-1} + \ldots + P_{\nu-1} V + P_\nu,$$

$$\frac{1}{(V - V_\rho)^r} = \frac{1}{V^r} + \frac{r}{1} \frac{V_\rho}{V^{r+1}} + \frac{r(r+1)}{1.2} \frac{V_\rho^2}{V^{r+2}} + \ldots$$

et en négligeant dans le produit les puissances négatives de V. En comparant le résultat obtenu avec la formule (12), on obtient

$$(14)\quad \left\{\begin{aligned}
\theta_0 &= P_{\nu-r} + \frac{r}{1} P_{\nu-r-1} V_\rho + \frac{r(r+1)}{1.2} P_{\nu-r-2} V_\rho^2 + \ldots \\
&\quad + \frac{r(r+1)\ldots(\nu-1)}{1.2\ldots(\nu-r-1)} V_\rho^{\nu-r}, \\
\theta_1 &= P_{\nu-r-1} + \frac{r}{1} P_{\nu-r-2} V_\rho + \ldots \\
&\quad + \frac{r(r+1)\ldots(\nu-2)}{1.2\ldots(\nu-r-2)} V_\rho^{\nu-r-1}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
\theta_{\nu-r-2} &= P_2 + \frac{r}{1} P_1 V_\rho + \frac{r(r+1)}{1.2} V_\rho^2, \\
\theta_{\nu-r-1} &= P_1 + \frac{r}{1} V_\rho.
\end{aligned}\right.$$

D'après ces formules (14) et en se servant des formules (6), on trouve que le numérateur de l'expression (13) de Y_ρ est le produit du polynôme

$$(15)\quad \left\{\begin{aligned}
&(\nu-1)\ldots(\nu-r)s_0 V_\rho^{\nu-r} \\
&\quad + (\nu-2)\ldots(\nu-r-1)s_1 V_\rho^{\nu-r-1} + \ldots \\
&\quad + r(r-1)\ldots 2 s_{\nu-r}
\end{aligned}\right.$$

par le facteur numérique $\frac{1}{1.2.3\ldots(r-1)}$; on voit que cette expression (15) est précisément la valeur que prend pour $V = V_\rho$ la dérivée d'ordre $r-1$, $\Theta^{r-1}(V)$, du polynôme $\Theta(V)$. Quant au dénominateur de l'expression de Y_ρ, il est égal à $\varphi(V_\rho)$ ou à

$$\frac{\psi^r(V_\rho)}{1.2.3\ldots r}.$$

La formule (13) devient alors

$$(16) \qquad \frac{1}{r} Y_\rho = \frac{\Theta^{r-1}(V_\rho)}{\psi^r(V_\rho)};$$

dans le cas de $r=1$, Y_ρ doit être remplacé par y_ρ et $\Theta^{r-1}(V_\rho)$ par $\Theta(V_\rho)$; on retombe ainsi sur celle des formules (8) qui détermine y_ρ.

La formule (16) exprime ce résultat remarquable, que l'expression générale

$$y = \frac{\Theta(V)}{\psi'(V)}$$

convient à tous les cas, pourvu que, si le second membre se réduit à $\frac{0}{0}$ pour $V=V_\rho$, on supprime les facteurs $V-V_\rho$ communs aux deux termes, avant de faire $V=V_\rho$, et qu'on remplace y par la moyenne arithmétique des valeurs qui répondent à la valeur V_ρ.

Soient

$$y_0,\ y_1,\ y_2,\ \ldots,\ y_{r-1}$$

les r valeurs de y qui répondent à la valeur V_ρ, la méthode que nous avons développée nous permet de calculer la somme

$$y_0 + y_1 + y_2 + \ldots + y_{r-1}.$$

On pourra aussi calculer, de la même manière, la somme des carrés de ces quantités, la somme de leurs cubes, etc., et enfin la somme de leurs puissances $r^{\text{ièmes}}$; on pourra donc former l'équation de degré r, qui a pour racines les quantités $y_0, y_1, \ldots, y_{r-1}$. Ainsi, quand l'équation en V a des racines égales, la détermination de la fonction y peut dépendre d'une équation du deuxième, ou du troisième, etc., degré.

500. L'analyse qui précède peut être étendue au cas où la fonction y n'admet pas toutes les substitutions de la fonction donnée V.

Dans ce cas, le nombre ν des valeurs distinctes de V est moindre que $N = 1.2...n$; et si l'on pose

$$N = \mu\nu,$$

les N valeurs de V se partageront en ν groupes contenant chacun μ valeurs égales. Soient

$$\begin{matrix} V_0, & V_0^{(1)}, & \ldots, & V_0^{(\mu-1)}, \\ V_1, & V_1^{(1)}, & \ldots, & V_1^{(\mu-1)}, \\ \ldots, & \ldots, & \ldots, & \ldots, \\ V_{\nu-1}, & V_{\nu-1}^{(1)}, & \ldots, & V_{\nu-1}^{(\mu-1)} \end{matrix}$$

ces ν groupes, et $y_\rho^{(\sigma)}$ la valeur de y qui correspond à $V_\rho^{(\sigma)}$.

Désignons par z une fonction symétrique et rationnelle quelconque des quantités

$$y_\rho, \; y_\rho^{(1)}, \; \ldots, \; y_\rho^{(\mu-1)},$$

il est évident que la fonction z admettra toutes les substitutions de V_ρ; on pourra donc exprimer z, en général, par une fonction rationnelle de V_ρ. Quand on aura ainsi calculé μ fonctions symétriques des quantités $y_\rho, y_\rho^{(1)}, \ldots, y_\rho^{(\mu-1)}$, on pourra former l'équation du degré μ, qui a pour racines ces μ valeurs de y.

501. On voit, par ce qui précède, qu'on pourra toujours déterminer les n racines $x_0, x_1, \ldots, x_{n-1}$ d'une équation donnée du degré n, si l'on connaît la valeur d'une fonction V de ces racines, pourvu que les $1.2.3\ldots n$ valeurs que prend V, quand on y permute les racines, soient différentes, non-seulement sous le rapport de la forme algébrique, mais encore au point de vue numérique.

En effet, on peut supposer que la fonction inconnue y

se réduise à l'une quelconque des racines, à x_0 par exemple; alors on pourra exprimer x_0 en fonction rationnelle de V et des coefficients de l'équation proposée. Si ensuite on suppose que y se réduise à une autre racine x_1, on pourra de même exprimer x_1 en fonction rationnelle de V, et ainsi de suite. Il résulte de là que si la valeur donnée de V est commensurable, c'est-à-dire exprimable en fonction rationnelle des quantités que l'on regarde comme connues, les racines de l'équation proposée seront toutes commensurables.

Mais, si la fonction V n'a pas toutes ses valeurs distinctes, qu'elle prenne, par exemple, k valeurs égales par les substitutions auxquelles répondent les valeurs

$$x_0, x_1, \ldots, x_{k-1}$$

de la fonction $y = x$, la méthode précédente ne fera plus connaître ces racines, elle permettra seulement de former l'équation du $k^{\text{ième}}$ degré dont elles dépendent.

La théorie qui vient d'être exposée comprend tout ce que l'on sait de plus général sur l'abaissement des équations quand on connaît une relation entre les racines, car ce cas est évidemment le même que celui où l'on donne la valeur d'une fonction des racines.

Recherches de Galois relatives à la théorie précédente.

502. L'analyse que nous venons de présenter nous a conduit à un théorème dont on comprend toute l'importance et que l'on peut énoncer comme il suit :

THÉORÈME. — *Si*

$$(1) \qquad f(x) = 0$$

est une équation quelconque de degré n, mais qui n'a pas de racines égales, et que

$$V = \varphi(x_0, x_1, \ldots, x_{n-1})$$

soit une fonction rationnelle des racines $x_0, x_1, \ldots, x_{n-1}$ *de l'équation* (1), *tellement choisie, que les* 1.2.3...*n valeurs qu'elle prend, par les substitutions des racines, soient toutes différentes, on pourra exprimer ces n racines* $x_0, x_1, \ldots, x_{n-1}$ *en fonction rationnelle de* V.

Il ne sera pas inutile de faire connaître ici la démonstration que Galois a donnée de ce théorème dans le célèbre Mémoire inséré au tome XI du *Journal de Mathématiques pures et appliquées*.

Nous désignerons par V_0 la valeur donnée de V, et par

$$V_0, \ V_1, \ \ldots, \ V_{\mu-1}$$

les $\mu = 1.2.3\ldots(n-1)$ valeurs que prend V, par les substitutions des $n-1$ racines

$$x_1, \ x_2, \ \ldots, \ x_{n-1}.$$

On aura alors une équation en V du degré μ, savoir

$$(2) \qquad (V - V_0)(V - V_1)\ldots(V - V_{\mu-1}) = 0,$$

dont les racines $V_0, V_1, \ldots$ seront toutes différentes et dont les coefficients, qui sont des fonctions symétriques des racines $x_1, x_2, \ldots, x_{n-1}$ de l'équation

$$\frac{f(x)}{x - x_0} = 0,$$

s'exprimeront rationnellement par les coefficients de cette équation, c'est-à-dire en fonction rationnelle de x_0 et des coefficients de l'équation proposée (1). Par suite, l'équation (2) pourra être mise sous la forme

$$(3) \qquad F(V, x_0) = 0,$$

F désignant une fonction rationnelle de V et de x_0. Or l'équation (2) ou (3) est satisfaite pour $V = V_0$; on aura

donc identiquement

$$F(V_0, x_0) = 0,$$

en sorte que l'équation

(4) $$F(V_0, x) = 0$$

sera satisfaite en posant

$$x = x_0,$$

et, en conséquence, les équations (1) et (4) auront une racine commune x_0. Je dis, de plus, que ces équations ne sauraient avoir d'autre racine commune. Supposons, en effet, que l'équation (4) soit satisfaite pour $x = x_1$, on aura identiquement

$$F(V_0, x_1) = 0;$$

par suite, l'équation

(5) $$F(V, x_1) = 0$$

sera satisfaite pour $V = V_0$. Or l'équation (5) se déduit de l'équation (3), ou de l'équation (2), par la transposition des racines x_0 et x_1; d'ailleurs, par cette transposition, les quantités $V_0, V_1, \ldots, V_{\mu-1}$ se changent en d'autres $V'_0, V'_1, \ldots, V'_{\mu-1}$, toutes distinctes des premières par hypothèse; donc l'équation (5) peut se mettre sous la forme

$$(V - V'_0)(V - V'_1)\ldots(V - V'_{\mu-1}) = 0,$$

et l'on voit qu'elle ne saurait avoir V_0 pour racine.

Les équations (1) et (4) n'ayant que la seule racine commune x_0, on déterminera facilement cette racine. Pour cela on cherchera le plus grand commun diviseur entre $f(x)$ et $F(V_0, x)$, et l'on poussera l'opération jusqu'à ce qu'on obtienne un reste du premier degré en x : en égalant à zéro ce reste, on aura une équation qui fera connaître la valeur de x_0,

$$x_0 = \psi(V_0) \quad \text{ou} \quad x_0 = \psi(V):$$

et cette valeur de x_0 sera évidemment rationnelle en V, puisque l'opération du plus grand commun diviseur ne peut pas introduire de radicaux.

On peut opérer de la même manière pour trouver les autres racines, et l'on obtiendra ainsi des expressions rationnelles, telles que

$$x_0 = \psi_0(V), \quad x_1 = \psi_1(V), \quad \ldots, \quad x_{n-1} = \psi_{n-1}(V).$$

Corollaire I. — *L'équation V du degré N = 1.2.3...n, qui a pour racines toutes les N valeurs de V et dont les coefficients s'expriment rationnellement par ceux de l'équation proposée, jouit de cette propriété remarquable que toutes ses racines peuvent être exprimées rationnellement par l'une quelconque d'entre elles.*

Soient, en effet, V et V_1 deux valeurs de V; V_1 est une fonction rationnelle des racines $x_0, x_1, \ldots, x_{n-1}$, lesquelles, d'après ce qui précède, sont des fonctions rationnelles de V : on aura donc

$$V_1 = \Theta(V),$$

Θ désignant une fonction rationnelle.

Corollaire II. — *Étant données tant d'irrationnelles algébriques qu'on voudra, on peut toujours les exprimer toutes en fonction rationnelle d'une même irrationnelle.*

Nous nommons irrationnelle algébrique toute quantité qui est racine d'une équation algébrique dont les coefficients sont des fonctions rationnelles des quantités regardées comme connues. Cela étant, soient

$$x_0, \quad x_1, \quad \ldots, \quad x_{m-1}$$

m irrationnelles algébriques quelconques; on pourra former une équation d'un certain degré n, à coefficients commensurables, dont ces m quantités seront racines,

et qui n'aura pas de racines égales. Soient

$$x_0, x_1, \ldots, x_{n-1}$$

les n racines de cette équation, et désignons par V une fonction rationnelle de ces n racines telle, que les valeurs qu'elle prend par les substitutions soient toutes distinctes : V sera une irrationnelle algébrique en fonction de laquelle les m irrationnelles données pourront s'exprimer rationnellement, d'après le théorème précédent

Nous admettons comme évident qu'on peut toujours former une fonction rationnelle de m quantités inégales, telle que les $1.2.3\ldots m$ valeurs qu'on en déduit par les substitutions soient différentes.

503. Application a un exemple. — Le théorème précédent fournit une méthode beaucoup plus simple que celle qui résulte de la théorie de Lagrange, pour déterminer les racines d'une équation quand on se donne une fonction de ces racines. Nous prendrons comme exemple le cas de l'équation du troisième degré.

Soit l'équation

$$x^3 + p_1 x^2 + p_2 x + p_3 = 0, \tag{1}$$

et posons

$$V = a x_0 + b x_1 + c x_2.$$

En transposant les lettres x_1 et x_2, on obtient ces deux valeurs de V,

$$V_0 = a x_0 + b x_1 + c x_2,$$
$$V_1 = a x_0 + b x_2 + c x_1;$$

l'équation en V sera alors

$$(V - V_0)(V - V_1) = 0,$$

ou

$$\begin{aligned} V^2 &- [2 a x_0 + (b + c)(x_1 + x_2)]V \\ &+ [a^2 x_0^2 + a(b + c) x_0 (x_1 + x_2) + bc(x_1^2 + x_2^2) + (b^2 + c^2) x_1 x_2] = 0. \end{aligned}$$

On peut chasser x_1 et x_2 de cette équation à l'aide des relations

$$x_1 + x_2 = -p_1 - x_0,$$
$$x_1 x_2 = p_2 - x_0(x_1 + x_2) = p_2 + p_1 x_0 + x_0^2,$$
$$x_1^2 + x_2^2 = (p_1^2 - 2p_2) - x_0^2,$$

et l'on aura

$$(2)\quad \left\{ \begin{aligned} & V^2 - [(2a - b - c)x_0 - p_1(b + c)]V \\ & + [(a^2 + b^2 + c^2 - ab - ac - bc)x_0^2 \\ & + (b^2 + c^2 - ab - ac)p_1 x_0 + bcp_1^2 - (b - c)^2 p_2] = 0. \end{aligned} \right.$$

Il faudra maintenant, pour avoir x_0, faire $x = x_0$ dans le premier membre de l'équation (1) et chercher le plus grand commun diviseur entre le polynôme que l'on obtiendra ainsi et le premier membre de l'équation (2) : il n'y a même aucun calcul à faire dans le cas particulier où l'on a

$$a^2 + b^2 + c^2 - ab - ac - bc = 0;$$

car l'équation (2) ne contient plus alors que la première puissance de x_0, et elle en fait connaître immédiatement la valeur. Ce cas simple se présente si l'on prend pour a, b, c les trois racines cubiques de l'unité.

Soit α une racine cubique imaginaire de l'unité, et posons

$$a = 1, \quad b = \alpha, \quad c = \alpha^2,$$

on aura, à cause de $\alpha^2 + \alpha + 1 = 0$,

$$x_0 = \frac{V^2 - p_1 V + (p_1^2 - 3p_2)}{3V}.$$

504. Le théorème démontré au n° **502** a pour complément la proposition suivante, qui n'a pas moins d'importance dans la théorie des équations :

THÉORÈME. — *Soient*

$$(1) \qquad f(x) = 0$$

e équation de degré n qui n'a pas de racines égales,

$$V = \varphi(x_0, x_1, \ldots, x_{n-1})$$

e fonction rationnelle des racines $x_0, x_1, \ldots, x_{n-1}$ des quantités connues, tellement choisie, que les $= 1.2.3\ldots n$ fonctions qu'on en déduit par les sub- tutions des racines aient des valeurs numériques iné- les. Soient aussi

)
$$\mathfrak{F}(V) = 0$$

quation de degré N qui a pour racines les N valeurs V, F(V) un diviseur irréductible de degré ν du lynôme $\mathfrak{F}(V)$; désignons enfin les racines de l'équa- n

$$F(V) = 0$$

$$V_0,\ V_1,\ V_2,\ \ldots,\ V_{\nu-1}.$$

les racines de l'équation proposée (1) *sont repré- tées par*

$$\psi_0(V_0),\ \psi_1(V_0),\ \ldots,\ \psi_{n-1}(V_0),$$

s pourront l'être aussi par

$$\psi_0(V_i),\ \psi_1(V_i),\ \ldots,\ \psi_{n-1}(V_i),$$

désignant l'une quelconque des quantités (5).

En effet, l'équation (1) admet par hypothèse la racine V_0); on a donc $f\,\psi_k(V_0) = 0$, et, par conséquent, est racine de l'équation

$$f\psi_k(V) = 0.$$

V_0 est l'une des racines de l'équation (4) et, comme le-ci est irréductible, toutes ses racines doivent satis-

faire à l'équation précédente : on a donc $f\psi_k(V_i) = 0$, ce qui exprime que les quantités (7) sont racines de l'équation (1).

Pour achever la démonstration du théorème énoncé, il reste à prouver que les quantités (7) sont distinctes. Je dis qu'on ne peut pas avoir $\psi_k(V_i) = \psi_j(V_i)$, si j est différent de k ; en effet, si cette égalité avait lieu, V_i serait racine de l'équation

$$\psi_k(V) - \psi_j(V) = 0,$$

laquelle admettrait alors chacune des racines (5) de l'équation irréductible (4); on aurait donc en particulier $\psi_k(V_0) - \psi_j(V_0) = 0$, ce qui est contre l'hypothèse.

Corollaire. — *Les substitutions* $1, S_1, S_2, \ldots, S_{\nu-1}$, *par lesquelles on passe de la permutation* (6) *des racines* $x_0, x_1, \ldots, x_{n-1}$ *aux* ν *permutations* (7), *forment un système conjugué. En d'autres termes, les* ν *permutations* (7) *constituent un groupe.*

En effet, on a $V_i = \theta(V_0)$, θ étant une fonction rationnelle; il s'ensuit que V_0 est racine de $F\theta(V) = 0$: cette équation admet donc la racine V_j, et $\theta(V_j)$ est l'une des racines V_k de l'équation (4). Cela posé, désignons par A_i la permutation (7), on aura

$$S_i A_0 = A_i = \psi_0\theta(V_0), \quad \psi_1\theta(V_0), \quad \ldots, \quad \psi_{n-1}\theta(V_0),$$

et, en faisant la substitution S_j,

$$\begin{aligned} S_j S_i A_0 &= \psi_0\theta(V_j), \ \psi_1\theta(V_j), \ \ldots, \ \psi_{n-1}\theta(V_j) \\ &= \psi_0(V_k), \ \psi_1(V_k), \ \ldots, \ \psi_{n-1}(V_k) = S_k A_0, \end{aligned}$$

d'où

$$S_j S_i = S_k.$$

SECTION V.

LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS.

SECTION V.

LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS.

CHAPITRE PREMIER.

DES ÉQUATIONS DU TROISIÈME ET DU QUATRIÈME DEGRÉ. CONSIDÉRATIONS GÉNÉRALES SUR LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS.

Résolution de l'équation générale du troisième degré.

505. Méthode de Hudde. — Parmi les méthodes connues pour la résolution de l'équation générale du troisième degré, la plus simple est, sans contredit, celle de Hudde; c'est aussi celle que nous exposerons la première.

Comme on peut toujours faire disparaître le deuxième terme d'une équation, nous considérerons l'équation

$$(1) \qquad x^3 + px + q = 0$$

débarrassée du terme en x^2. Posons

$$(2) \qquad x = y + z,$$

y étant une nouvelle variable et z une fonction de y, que nous nous réservons de déterminer, de manière que l'équation transformée en y rentre, s'il est possible, dans les classes d'équations que nous savons résoudre. Remplaçons dans l'équation (1) x par sa valeur tirée de (2), on aura

$$(y+z)^3 + p(y+z) + q = 0,$$

ou

$$(3) \qquad (y^3 + z^3 + q) + (y + z)(3yz + p) = 0.$$

Si maintenant on détermine z par la condition

$$3yz + p = 0,$$

ce qui donne

$$z = -\frac{p}{3y},$$

l'équation (3) deviendra

$$y^3 - \frac{p^3}{27y^3} + q = 0,$$

ou

$$(4) \qquad y^6 + qy^3 - \frac{p^3}{27} = 0.$$

Cette équation en y peut se résoudre à la manière des équations du deuxième degré, car elle ne contient que les puissances y^3 et y^6. Ensuite, quand y sera connu, on aura x par la formule

$$(5) \qquad x = y - \frac{p}{3y}.$$

L'équation du sixième degré (4), à laquelle nous ramenons ainsi l'équation proposée, a été nommée par Lagrange la *réduite* ou la *résolvante* de l'équation (1).

Quoique cette résolvante ait six racines, la formule (5) ne donnera pourtant que trois valeurs de x, comme cela doit être. En effet, la résolvante ne change pas quand on change y en $-\frac{p}{3y}$, en sorte que ses six racines forment trois groupes tels, que le produit des deux racines de chaque groupe est égal à $-\frac{p}{3}$, et il est évident que la formule (5) donnera la même valeur pour x quand on remplacera y successivement par les deux racines d'un même groupe. Cela va résulter, au surplus, de l'ex-

pression même des valeurs de x dont nous allons nous occuper.

De l'équation (4) on tire cette valeur de y^3,

$$y^3 = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

ou

(6) $$y^3 = -\frac{q}{2} \pm \sqrt{R},$$

en faisant, pour abréger,

$$R = \frac{q^2}{4} + \frac{p^3}{27};$$

enfin, on tire de l'équation (6)

(7) $$y = \sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}.$$

Cette expression, à cause des valeurs multiples des radicaux, donne les six racines de l'équation (4); mais nous admettrons, dans ce qui va suivre, que $\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}$ représentera seulement l'une des trois racines cubiques de $-\frac{q}{2} \pm \sqrt{R}$: ce sera celle que l'on voudra, mais ce sera toujours la même; en sorte que, si α et β désignent les deux racines cubiques imaginaires de l'unité, les six racines de l'équation (4) pourront être représentées par

(8) $$\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}},\quad \alpha\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}},\quad \beta\sqrt[3]{-\frac{q}{2} \pm \sqrt{R}}.$$

Et comme, des deux radicaux

$$\sqrt[3]{-\frac{q}{2} + \sqrt{R}},\quad \sqrt[3]{-\frac{q}{2} - \sqrt{R}},$$

le premier nous représente, par notre convention, celle

celles du second seront

$$B,\ B\alpha,\ B\beta;$$

et, comme les valeurs des deux radicaux qu'il faut prendre ensemble doivent avoir un produit réel, on aura, pour les racines de l'équation (1),

$$A+B,$$
$$A\alpha+B\beta,$$
$$A\beta+B\alpha.$$

D'ailleurs,

$$\alpha=\frac{-1+\sqrt{-3}}{2},\quad \beta=\frac{-1-\sqrt{-3}}{2};$$

les trois racines de l'équation (1) seront donc

$$A+B \quad \text{et} \quad -\frac{A+B}{2}\pm\frac{A-B}{2}\sqrt{-3}.$$

Ainsi, dans ce cas, l'équation (1) a deux racines imaginaires.

Si l'on a $R=0$, ou

$$4p^3+27q^2=0,$$

il en résulte $B=A$; alors l'équation (1) a ses trois racines réelles, mais deux de ces racines sont égales entre elles.

Supposons, enfin, $R<0$, ou

$$4p^3+27q^2<0;$$

chacun des radicaux qui figurent dans la valeur de x aura ses trois valeurs imaginaires; mais il est facile de voir que l'équation (1) a ses racines réelles et inégales. Soient, en effet,

$$A+B\sqrt{-1},\quad \alpha(A+B\sqrt{-1}),\quad \beta(A+B\sqrt{-1})$$

les trois racines cubiques de l'expression imaginaire $-\frac{q}{2}+\sqrt{R}$; l'expression imaginaire conjuguée $-\frac{q}{2}-\sqrt{R}$ aura évidemment pour racines cubiques

$$A - B\sqrt{-1},\quad 6(A - B\sqrt{-1}),\quad \alpha(A - B\sqrt{-1});$$

et, comme les valeurs des deux radicaux qui composent la valeur (10) de x doivent avoir un produit réel, on aura les trois valeurs suivantes de x :

$$(A + B\sqrt{-1}) + (A - B\sqrt{-1}),$$
$$\alpha(A + B\sqrt{-1}) + 6(A - B\sqrt{-1}),$$
$$6(A + B\sqrt{-1}) + \alpha(A - B\sqrt{-1});$$

ou, en remplaçant α et 6 par leurs valeurs,

$$2A,\quad -A + B\sqrt{3},\quad -A - B\sqrt{3}.$$

L'équation (1) a donc ses trois racines réelles, comme nous l'avions annoncé, et il est très-facile de montrer qu'elles sont inégales.

En effet, on ne peut avoir d'abord

$$-A + B\sqrt{3} = -A - B\sqrt{3},$$

car il en résulterait $B = 0$, et la quantité $-\frac{q}{2}+\sqrt{R}$ serait égale à la quantité réelle A^3, ce qui est contre l'hypothèse. On ne peut avoir non plus

$$2A = -A \pm B\sqrt{3},$$

car il en résulterait $B = \pm A\sqrt{3}$; par suite,

$$A + B\sqrt{-1} = A(1 \pm \sqrt{-3}) = -2\alpha A,$$

et

$$-\frac{q}{2}+\sqrt{R} = -8\alpha^3A^3 = -8A^3,$$

ce qui est encore contre l'hypothèse, puisque le second membre est réel.

Le cas que nous examinons ici est fort remarquable : car, bien qu'alors les trois racines de l'équation du troisième degré soient réelles, la formule de Cardan présente leurs valeurs sous une forme compliquée d'imaginaires ; et si, pour faire disparaître ces imaginaires, on cherchait à mettre les radicaux cubiques qui entrent dans la formule de Cardan sous la forme $A + B\sqrt{-1}$, on trouverait que les quantités A et B dépendent d'une équation toute semblable à la proposée. L'équation en A, par exemple, aurait ses trois racines réelles, et l'on trouverait, par conséquent, une expression de A également compliquée d'imaginaires. C'est pour cette raison que le cas dont il s'agit ici a été nommé *cas irréductible*.

507. Ainsi la formule de Cardan ne peut servir à la résolution *numérique* de l'équation du troisième degré que si une seule racine est réelle ; mais, dans le cas irréductible, l'équation se résout très-simplement par le moyen des fonctions circulaires. Si l'on pose, en effet,

$$\frac{q^2}{4} + \frac{p^3}{27} = -\rho^2 \sin^2\omega, \quad -\frac{q}{2} = \rho\cos\omega,$$

la quantité ρ et l'angle ω seront déterminés par les formules

$$\rho = \sqrt{\frac{-p^3}{27}}, \quad \cos\omega = \frac{-\frac{q}{2}}{\sqrt{\frac{-p^3}{27}}},$$

et la formule de Cardan donnera

$$x = \sqrt[3]{\rho}\left(\sqrt[3]{\cos\omega + \sqrt{-1}\sin\omega} + \sqrt[3]{\cos\omega - \sqrt{-1}\sin\omega}\right),$$

$\sqrt[3]{\rho}$ désignant une quantité réelle; on a d'ailleurs

$$\sqrt[3]{\cos\omega - \sqrt{-1}\sin\omega} = \cos\frac{\omega + 2k\pi}{3} - \sqrt{-1}\sin\frac{\omega + 2k\pi}{3},$$

$$\sqrt[3]{\cos\omega + \sqrt{-1}\sin\omega} = \cos\frac{\omega + 2k\pi}{3} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{3},$$

où k a l'une des trois valeurs 0, 1, 2. On doit donner à k la même valeur dans ces deux formules, car il faut que le produit de leurs premiers membres soit réel; on aura donc

$$x = 2\sqrt[3]{\rho}\cos\frac{\omega + 2k\pi}{3},$$

et les trois racines de l'équation seront

$$2\sqrt[3]{\rho}\cos\frac{\omega}{3},\quad 2\sqrt[3]{\rho}\cos\frac{\omega + 2\pi}{3},\quad 2\sqrt[3]{\rho}\cos\frac{\omega + 4\pi}{3}.$$

On pourra, dans chaque cas, calculer par logarithmes les trois racines dont nous venons de donner l'expression.

508. Méthode de Lagrange. — Considérons l'équation complète du troisième degré

$$(1)\qquad x^3 + Px^2 + Qx + R = 0,$$

et désignons par x_0, x_1, x_2 ses trois racines. D'après la théorie exposée aux nos 501 et 502, on pourra déterminer les racines x_0, x_1, x_2, si l'on parvient à connaître la valeur d'une fonction quelconque de ces racines, tellement choisie, cependant, que les six valeurs qu'elle peut prendre par les 1.2.3 substitutions de x_0, x_1, x_2 soient différentes. La méthode de Lagrange, que nous allons exposer ici, consiste à déterminer directement la valeur d'une fonction linéaire des trois racines, telle que

$$(2)\qquad t = x_0 + Ax_1 + Bx_2,$$

où A et B désignent des constantes quelconques, et à déduire ensuite de cette fonction l'expression des racines elles-mêmes.

Si l'on exécute sur les indices 0, 1, 2 toutes les substitutions qu'ils comportent, on obtiendra les six valeurs suivantes de la fonction t :

$$(3)\quad \begin{cases} t_0 = x_0 + Ax_1 + Bx_2, \\ t_1 = x_0 + Ax_2 + Bx_1, \\ t_2 = x_1 + Ax_2 + Bx_0, \\ t_3 = x_1 + Ax_0 + Bx_2, \\ t_4 = x_2 + Ax_0 + Bx_1, \\ t_5 = x_2 + Ax_1 + Bx_0, \end{cases}$$

et cette fonction t dépendra de l'équation du sixième degré

$$(4)\quad (t-t_0)(t-t_1)(t-t_2)(t-t_3)(t-t_4)(t-t_5) = 0,$$

que l'on ramènera au deuxième degré, si l'on peut disposer des constantes indéterminées A et B, de manière qu'elle ne renferme que la sixième et la troisième puissance de t. Il faut et il suffit, pour qu'il en soit ainsi, que, t désignant l'une quelconque des racines de l'équation (4), α une racine cubique imaginaire de l'unité, αt et $\alpha^2 t$ soient aussi racines de l'équation (4). Voyons si cette condition peut être remplie. D'abord αt_0 et $\alpha^2 t_0$ ne peuvent être égaux ni à t_1, ni à t_3, ni à t_5, lorsqu'on regarde x_0, x_1, x_2 comme des indéterminées, car autrement on aurait $\alpha = 1$; il faut donc que l'on ait

$$\alpha t_0 = t_2 \quad \text{et} \quad \alpha^2 t_0 = t_4,$$

ou

$$\alpha t_0 = t_4 \quad \text{et} \quad \alpha^2 t_0 = t_2.$$

Ces deux dernières équations équivalent aux précédentes, puisque rien ne distingue les racines α et α^2 l'une de

l'autre; nous adopterons les précédentes, et comme celles-ci doivent avoir lieu, quelles que soient x_0, x_1, x_2, nous en déduirons les valeurs suivantes de A et de B:

$$A = \alpha, \quad B = \alpha^2.$$

Il arrive alors que, A et B ayant ces valeurs, on a aussi

$$\alpha t_1 = t_3, \quad \alpha^2 t_1 = t_5,$$

en sorte que, si l'on prend pour valeur de t

$$t = x_0 + \alpha x_1 + \alpha^2 x_2,$$

l'équation en t aura pour racines

$$t_0, \ \alpha t_0, \ \alpha^2 t_0, \ t_1, \ \alpha t_1, \ \alpha^2 t_1,$$

et elle sera, par conséquent,

$$(t^3 - t_0^3)(t^3 - t_1^3) = 0,$$

où

(5) $$t^6 - (t_0^3 + t_1^3)t^3 + t_0^3 t_1^3 = 0,$$

en faisant

(6) $$\begin{cases} t_0 = x_0 + \alpha x_1 + \alpha^2 x_2, \\ t_1 = x_0 + \alpha^2 x_1 + \alpha x_2; \end{cases}$$

ce qui s'accorde avec les résultats généraux que nous avons obtenus au n° 494.

Lorsque les valeurs de t_0 et t_1 seront connues, celles de x_0, x_1, x_2 le seront aussi; on a, en effet,

(7) $$-P = x_0 + x_1 + x_2,$$

et, en ajoutant les équations (6) et (7), il vient, à cause de $\alpha^2 + \alpha + 1 = 0$,

(8) $$x_0 = \frac{-P + t_0 + t_1}{3}.$$

Pour avoir x_1, il faut ajouter les trois équations (6) et (7),

après les avoir multipliées respectivement par α^2, α et 1; on a ainsi

$$(9)\qquad x_1 = \frac{-P + \alpha^2 t_0 + \alpha t_1}{3},$$

et enfin on obtient la valeur suivante de x_2,

$$(10)\qquad x_2 = \frac{-P + \alpha t_0 + \alpha^2 t_1}{3},$$

en ajoutant les équations (6) et (7), après les avoir respectivement multipliées par α, α^2 et 1.

Tout est donc ramené à résoudre l'équation (5), qui est alors une *réduite* ou une *résolvante* de l'équation proposée. Cherchons d'abord à exprimer les coefficients de la résolvante par ceux de l'équation proposée, ce qui est possible, puisque ces coefficients $t_0^3 + t_1^3$ et $t_0^3 t_1^3$ sont des fonctions symétriques des racines.

Si l'on multiplie les deux équations (6) l'une par l'autre, et qu'on ait égard à la relation $\alpha^2 + \alpha + 1 = 0$, il vient

$$\begin{aligned} t_0 t_1 &= x_0^2 + x_1^2 + x_2^2 - x_0 x_1 - x_1 x_2 - x_2 x_0 \\ &= (x_0 + x_1 + x_2)^2 - 3(x_0 x_1 + x_1 x_2 + x_2 x_0); \end{aligned}$$

et, par conséquent,

$$(11)\qquad t_0 t_1 = P^2 - 3Q;$$

si, enfin, on ajoute les deux équations (6), après les avoir élevées au cube, on obtient

$$\begin{aligned} t_0^3 + t_1^3 &= 2(x_0^3 + x_1^3 + x_2^3) \\ &\quad - 3(x_0^2 x_1 + x_1^2 x_0 + x_1^2 x_2 + x_2^2 x_1 + x_2^2 x_0 + x_0^2 x_2) + 12 x_0 x_1 x_2 \\ &= 3(x_0^3 + x_1^3 + x_2^3) - (x_0 + x_1 + x_2)^3 + 18 x_0 x_1 x_2 \\ &= -2P^3 + 9PQ - 27R; \end{aligned}$$

la résolvante (5) devient donc

$$t^6 - (-2P^3 + 9PQ - 27R)t^3 + (P^2 - 3Q)^3 = 0.$$

En posant

$$t^3 = \theta,$$

elle se réduit à l'équation du deuxième degré

$$\theta^2 - (-2P^3 + 9PQ - 27R)\theta + (P^2 - 3Q)^3 = 0;$$

et, si l'on nomme θ_0 et θ_1 les deux racines de cette équation, on aura

$$t_0 = \sqrt[3]{\theta_0}, \quad t_1 = \sqrt[3]{\theta_1}.$$

Les équations (8), (9) et (10) deviennent alors

$$x_0 = \frac{-P + \sqrt[3]{\theta_0} + \sqrt[3]{\theta_1}}{3},$$

$$x_1 = \frac{-P + \alpha^2\sqrt[3]{\theta_0} + \alpha\sqrt[3]{\theta_1}}{3},$$

$$x_2 = \frac{-P + \alpha\sqrt[3]{\theta_0} + \alpha^2\sqrt[3]{\theta_1}}{3};$$

on prendra pour $\sqrt[3]{\theta_0}$ l'une quelconque des trois valeurs de ce radical, mais la même dans les trois formules : quant à l'autre radical $\sqrt[3]{\theta_1}$, sa valeur est déterminée quand on a fixé celle de $\sqrt[3]{\theta_0}$, car l'équation (11) nous donne

$$\sqrt[3]{\theta_0} \cdot \sqrt[3]{\theta_1} = P^2 - 3Q.$$

Il suit de là que les trois racines pourront être représentées par la formule unique

$$x = \frac{-P + \sqrt[3]{\theta_0} + \sqrt[3]{\theta_1}}{3},$$

qui n'a que trois valeurs distinctes, si l'on considère que $\sqrt[3]{\theta_1}$ y est mis, pour abréger, à la place de $\frac{P^2 - 3Q}{\sqrt[3]{\theta_0}}$.

509. Comparaison des deux méthodes précédentes. — La méthode de Lagrange, que nous venons d'exposer, est moins simple que celle de Hudde; mais elle est plus directe. Toutefois, ces deux méthodes fournissent la même résolvante, et nous allons voir qu'on est naturellement conduit à la méthode de Lagrange, en étudiant à fond celle de Hudde.

Reprenons l'équation générale du troisième degré

$$(1) \qquad x^3 + Px^2 + Qx + R = 0.$$

Pour appliquer la méthode de Hudde, on commence par faire disparaître le deuxième terme, en posant

$$x = -\frac{P}{3} + x',$$

ce qui ramène l'équation à la forme

$$(2) \qquad x'^3 + px' + q = 0;$$

on pose ensuite

$$x' = y - \frac{p}{3y},$$

et l'on obtient enfin cette résolvante,

$$(3) \qquad y^6 + qy^3 - \frac{p^3}{27} = 0.$$

Cela posé, si y_0 désigne l'une des trois racines cubiques de $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, y_1 celle des trois racines cubiques de $-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, qui, multipliée par y_0, donne pour produit $\frac{-p}{3}$, les six racines de l'équation (3) seront

$$y_0, \quad \alpha y_0, \quad \alpha^2 y_0, \quad y_1, \quad \alpha y_1, \quad \alpha^2 y_1,$$

et celles de l'équation (2)

$$y_0 + y_1, \quad \alpha y_0 + \alpha^2 y_1, \quad \alpha^2 y_0 + \alpha y_1;$$

par suite, en appelant x_0, x_1, x_2 les trois racines de l'équation (1), on aura

$$x_0 = -\frac{P}{3} + y_0 + y_1,$$

$$x_1 = -\frac{P}{3} + \alpha^2 y_0 + \alpha y_1,$$

$$x_2 = -\frac{P}{3} + \alpha y_0 + \alpha^2 y_1.$$

Si l'on ajoute ces équations, après les avoir respectivement multipliées d'abord par 1, α, α^2, puis ensuite par 1, α^2, α, il vient

$$y_0 = \frac{x_0 + \alpha x_1 + \alpha^2 x_2}{3},$$

$$y_1 = \frac{x_0 + \alpha^2 x_1 + \alpha x_2}{3}.$$

On voit par là que la méthode de Hudde revient, au fond, à former une résolvante en y dont la racine ait pour valeur

$$y = \frac{x_0 + \alpha x_1 + \alpha^2 x_2}{3},$$

et que cette résolvante ne diffère de celle de Lagrange que par le facteur 3 qui divise les racines.

510. Méthodes de Tschirnaüs et d'Euler. — Nous avons exposé au n° 190 la méthode générale de Tschirnaüs, pour faire disparaître d'une équation autant de termes que l'on veut. Il en résulte une méthode pour la résolution des équations du troisième degré; mais nous n'ajouterons rien ici à ce que nous avons dit à ce sujet au n° 191.

La méthode d'Euler ne diffère que dans la forme de celle de Tschirnaüs. Elle consiste à éliminer y entre deux équations de la forme

$$ay^2 + by + c = x, \quad y^3 = d,$$

et à identifier l'équation finale en x avec l'équation proposée; la résolution de celle-ci s'ensuivra évidemment. On peut disposer, à volonté, de la valeur de l'une des indéterminées a, b, c, d; on peut faire, par exemple, $a = 1$ ou $d = 1$.

Des équations du troisième degré dont deux racines peuvent s'exprimer rationnellement en fonction de la troisième racine et des quantités connues.

511. Si l'on désigne par x, x_1, x_2 les racines de l'équation du troisième degré

$$(1) \qquad x^3 + Px^2 + Qx + R = 0,$$

le produit

$$\Delta = (x - x_1)^2 (x - x_2)^2 (x_1 - x_2)^2$$

des carrés des différences des racines aura pour valeur (n° 179)

$$\Delta = -(4Q^3 + 27R^2) + 18PQR + P^2Q^2 - 4P^3R.$$

Cela posé, en multipliant par $x_1 - x_2$ l'identité

$$\sqrt{\Delta} = (x - x_1)(x - x_2)(x_2 - x_1),$$

il vient

$$(x_1 - x_2)\sqrt{\Delta} = [(x_1 - x)(x_1 - x_2)][(x_2 - x)(x_2 - x_1)]$$

ou

$$\begin{aligned}(x_1 - x_2)\sqrt{\Delta} &= (3x_1^2 + 2Px_1 + Q)(3x_2^2 + 2Px_2 + Q)\\ &= 9x_1^2x_2^2 + 6Px_1x_2(x_1 + x_2) + 3Q(x_1 + x_2)^2\\ &\quad + (4P^2 - 6Q)x_1x_2 + 2PQ(x_1 + x_2) + Q^2;\end{aligned}$$

on a d'ailleurs

$$(2)\qquad x_1 + x_2 = -x - P$$

ct

$$x_1 x_2 = -(x_1 + x_2)x + Q = x^2 + Px + Q;$$

en faisant usage de ces formules, on trouve

$$\begin{aligned}(x_1 - x_2)\sqrt{\Delta} = 9x^4 + 12Px^3 + (15Q + P^2)x^2 \\ + (10PQ - 2P^3)x + (4Q^2 - P^2Q).\end{aligned}$$

On peut ramener cette expression au deuxième degré, par le moyen de l'équation (1), et il vient alors

$$(3)\quad \left\{\begin{aligned}(x_1 - x_2)\sqrt{\Delta} = (6Q - 2P^2)x^2 - (9R - 7PQ + 2P^3)x \\ + (4Q^2 - P^2Q - 3PR).\end{aligned}\right.$$

On voit, par les équations (2) et (3), que les racines x_1 et x_2 seront égales aux deux valeurs de X tirées de la formule

$$(4)\quad \left\{\begin{aligned}X = \frac{1}{2\sqrt{\Delta}}\big[(6Q - 2P^2)x^2 - (9R - 7PQ + 2P^3 + \sqrt{\Delta})x \\ + (4Q^2 - P^2Q - 3PR - P\sqrt{\Delta})\big],\end{aligned}\right.$$

en y donnant successivement au radical $\sqrt{\Delta}$ ses deux valeurs.

Il résulte de là que, si l'on comprend ce radical $\sqrt{\Delta}$ parmi les quantités qu'on regarde comme connues, les racines x_1 et x_2 s'exprimeront par des fonctions rationnelles de x et des quantités connues.

On peut aussi représenter ces racines par des fonctions rationnelles et linéaires de x, en suivant la marche indiquée au n° 183. Effectivement, si l'on divise le premier nombre $F(x)$ de l'équation (1) par l'expression (4) de X, que l'on désigne par V le quotient de cette division et par $-U$ le reste, on aura

$$0 = F(x) = VX - U.$$

d'où

$$X = \frac{U}{V}.$$

On trouve, en faisant le calcul,

$$2\sqrt{\Delta}.V = (6Q - 2P^2)x + (9R - PQ + \sqrt{\Delta}),$$
$$2\sqrt{\Delta}.U = -(9R - PQ - \sqrt{\Delta})x + (2Q^2 \quad 6PR);$$

par conséquent, si l'on pose

$$(5) \quad \left\{ \begin{aligned} a &= \frac{\sqrt{\Delta} - (9R - PQ)}{2\sqrt{\Delta}}, \\ b &= \frac{2Q^2 - 6PR}{2\sqrt{\Delta}}, \\ a' &= \frac{6Q - 2P^2}{2\sqrt{\Delta}}, \\ b' &= \frac{\sqrt{\Delta} + (9R - PQ)}{2\sqrt{\Delta}}, \end{aligned} \right.$$

l'expression de X sera

$$X = \frac{ax + b}{a'x + b'},$$

et l'on en conclura les racines x_1 et x_2 en donnant au radical $\sqrt{\Delta}$ ses deux valeurs. Mais quand on change $\sqrt{\Delta}$ en $-\sqrt{\Delta}$, a et b' se changent l'une dans l'autre, tandis que b et a' se changent en $-b$ et $-a'$; donc on peut écrire

$$x_1 = \frac{ax + b}{a'x + b'}, \quad x_2 = \frac{b'x - b}{-a'x + a}.$$

On tire des équations (5)

$$(6) \qquad a + b' = 1, \quad ab' - ba' = 1,$$

et il en résulte que, si l'on pose

$$(7) \qquad \theta x = \frac{ax + b}{a'x + b'},$$

on aura

$$(8) \qquad \theta^2 x = \frac{b'x - b}{-a'x + a}, \quad \theta^3 x = x,$$

$\theta^2 x$, $\theta^3 x$ étant mis au lieu de $\theta\theta x$ et $\theta\theta^2 x$.

Les racines de l'équation proposée peuvent donc être représentées par

$$x,\ \theta x,\ \theta^2 x;$$

j'ajoute que, si une fonction linéaire

$$\varphi(x) = \frac{\alpha x + \beta}{\alpha' x + \beta'},$$

dont le déterminant $\alpha\beta' - \beta\alpha'$ peut toujours être supposé égal à 1, représente l'une des racines, θx par exemple, on aura identiquement

$$\varphi(x) = \theta x,$$

c'est-à-dire

$$\alpha = \pm a, \quad \beta = \pm b, \quad \alpha' = \pm a', \quad \beta' = \pm b'.$$

En effet, l'équation proposée étant irréductible, elle ne peut pas avoir une racine commune avec l'équation $\varphi x = \theta x$ qui est du deuxième degré, à moins que celle-ci ne soit identique.

512. Nous avons rencontré au n° **166** une équation du troisième degré dont les racines se développent en des fractions continues susceptibles d'être terminées par un même quotient complet.

L'analyse qui précède nous fait connaître toutes les équations du troisième degré qui possèdent cette propriété. En effet, pour que deux irrationnelles x et x_1 soient développables en des fractions continues terminées par les mêmes quotients, il faut et il suffit (n° **16**) que l'on ait

$$x_1 = \frac{ax + b}{a'x + b'},$$

a, b, a', b' étant des entiers positifs ou négatifs satisfaisant à la condition

$$ab' - ba' = \pm 1.$$

Si l'on applique ce résultat à deux des racines de l'équation (1), x et θx, ou x et $\theta^2 x$, on voit que la condition relative au déterminant est satisfaite quand on exprime θx ou $\theta^2 x$ par les formules (5), (7) et (8); donc, pour que les fractions continues dans lesquelles se développent les trois racines aient un même quotient complet commun, il faut et il suffit que les formules (5) donnent pour a, b, a', b' des valeurs entières.

Les deux dernières équations (5) peuvent être remplacées par les équations (6), et celles-ci donnent

$$(9) \qquad b' = 1 - a, \quad b = -\frac{1 - a + a^2}{a'};$$

en même temps on a, par les deux premières équations (5),

$$(10) \qquad 9R - PQ = (1 - 2a)\sqrt{\Delta}, \quad 3Q - P^2 = a'\sqrt{\Delta},$$

et l'expression de Δ peut être mise sous la forme

$$(11) \quad \begin{cases} 9\Delta = 3(9R - PQ)^2 + 4P(9R - PQ)(3Q - P^2) \\ \qquad\quad - 4Q(3Q - P^2)^2. \end{cases}$$

Des équations (10) et (11) on tire

$$(12) \quad \begin{cases} Q = -\dfrac{3(1 - a + a^2)}{a'^2} + \dfrac{1 - 2a}{a'}\,P, \\ R = \dfrac{(-1 + 2a)(1 - a + a^2)}{a'^3} + \dfrac{a(-1 + a)}{a'^2}\,P, \\ \sqrt{\Delta} = \dfrac{3Q - P^2}{a'}; \end{cases}$$

la quantité P demeure indéterminée.

D'après cela, la forme générale des équations dont nous nous occupons est

$$(13)\quad \begin{cases} x^3 + Px^2 + \left[\dfrac{-3(1-a+a^2)}{a'^2} + \dfrac{1-2a}{a'}P\right]x \\ + \left[\dfrac{(-1+2a)(1-a+a^2)}{a'^3} + \dfrac{a(-1+a)}{a'^2}P\right] = 0; \end{cases}$$

P désigne une quantité réelle quelconque, rationnelle ou irrationnelle ; a est un nombre entier positif ou négatif quelconque ; enfin a' est un diviseur positif ou négatif quelconque du nombre $1 - a + a^2$.

L'équation

$$x^3 - 7x + 7 = 0,$$

dont nous nous sommes occupé au n° 166, répond aux valeurs

$$P = 0, \quad a = -4, \quad a' = -3.$$

Résolution de l'équation générale du quatrième degré.

513. Méthode de Ferrari. — La méthode la plus simple pour résoudre l'équation du quatrième degré est aussi la plus ancienne ; c'est celle de Louis Ferrari : elle consiste à faire en sorte que les deux membres de l'équation soient des carrés, et elle ramène, en conséquence, la résolution de cette équation à celle de deux équations du deuxième degré.

Soit l'équation

$$(1)\qquad x^4 + px^3 + qx^2 + rx + s = 0;$$

en ne conservant dans le premier membre que les deux premiers termes, elle devient

$$x^4 + px^3 = -qx^2 - rx - s,$$

et, en ajoutant aux deux membres $\dfrac{p^2x^2}{4}$, afin que le pre-

mier membre devienne un carré,

$$(2) \qquad \left(x^2 + \frac{p}{2}x\right)^2 = \left(\frac{p^2}{4} - q\right)x^2 - rx - s.$$

Mise sous cette forme, l'équation proposée se résoudrait immédiatement, si le second membre était un carré; car il suffirait alors d'extraire la racine carrée des deux membres, et l'équation serait abaissée au deuxième degré. C'est à ce cas particulier que la méthode de Ferrari ramène tous les autres.

Désignons par y une quantité indéterminée, et ajoutons aux deux membres de l'équation (2) la même quantité

$$\left(x^2 + \frac{p}{2}x\right)y + \frac{y^2}{4},$$

il viendra

$$(3) \quad \left(x^2 + \frac{p}{2}x + \frac{y}{2}\right)^2 = \left(\frac{p^2}{4} - q + y\right)x^2 + \left(\frac{py}{2} - r\right)x + \left(\frac{y^2}{4} - s\right).$$

Maintenant, déterminons y, de manière que le second membre de l'équation (3) soit un carré. Il suffit, pour cela, que l'on ait

$$\left(\frac{py}{2} - r\right)^2 = \left(\frac{p^2}{4} - q + y\right)(y^2 - 4s),$$

ou

$$(4) \qquad y^3 - qy^2 + (pr - 4s)y - s(p^2 - 4q) - r^2 = 0;$$

et, si l'on connaît une seule racine de cette équation en y, la résolution de l'équation proposée (1) s'ensuivra immédiatement, car l'équation (3), qui est la même que (1), peut s'écrire comme il suit :

$$\left(x^2 + \frac{p}{2}x + \frac{y}{2}\right)^2 - \left(\frac{p^2}{4} - q + y\right)\left[x + \frac{p\frac{y}{2} - r}{2\left(\frac{p^2}{4} - q + y\right)}\right]^2 = 0.$$

et elle se décompose dans les deux suivantes, qui sont du deuxième degré :

$$\left\{\begin{aligned} &x^2+\left(\frac{p}{2}+\sqrt{\frac{p^2}{4}-q+y}\right)x+\left[\frac{y}{2}+\frac{\frac{py}{2}-r}{2\sqrt{\frac{p^2}{4}-q+y}}\right]=0,\\ &x^2+\left(\frac{p}{2}-\sqrt{\frac{p^2}{4}-q-y}\right)x+\left[\frac{y}{2}-\frac{\frac{py}{2}-r}{2\sqrt{\frac{p^2}{4}-q+y}}\right]=0. \end{aligned}\right.$$

L'équation (4), qui est du troisième degré, sera donc ici la *réduite* ou la *résolvante* de l'équation (1). Nous avons vu qu'on peut exprimer par des radicaux les racines de l'équation générale du troisième degré; il s'ensuit que l'équation du quatrième degré a la même propriété, car les équations (5) donneront les quatre racines de l'équation (1) en fonction des coefficients et d'une racine quelconque y de la résolvante.

514. Étude de la résolvante. — Nous venons de voir que les quatre racines de l'équation proposée peuvent s'exprimer en fonction d'une seule racine de la résolvante : nous allons étudier à son tour cette résolvante, et examiner de quelle manière ses racines sont composées avec celles de la proposée.

Désignons toujours par y une racine quelconque de la résolvante, et par x_0, x_1, x_2, x_3 les quatre racines de l'équation proposée, savoir, par x_0 et x_2 celles qui appartiennent à la première des équations (5); par x_1 et x celles qui appartiennent à la seconde. On aura alors

$$x_0x_2=\frac{y}{2}+\frac{\frac{py}{2}-r}{2\sqrt{\frac{p^2}{4}-q+y}},\quad x_1x_3=\frac{y}{2}-\frac{\frac{py}{2}-r}{2\sqrt{\frac{p^2}{4}-q+y}},$$

connaît la composition de ses racines; mais on peut aussi la déduire de la résolvante (3) en y. Il est facile, en effet, de voir que l'on a

$$y = \frac{\theta - p^2 + 4q}{4},$$

et la résolvante en θ est

$$(5)\quad \left\{\begin{array}{l} \theta^3 - (3p^2 - 8q)\theta^2 \\ \quad + (3p^4 - 16p^2q + 16q^2 + 16pr - 64s)\theta \\ \qquad\qquad - (p^3 - 4pq + 8r)^2 = 0. \end{array}\right.$$

On pourrait exprimer les quatre racines x_0, x_1, x_2, x_3 de la proposée par une seule des racines θ de cette équation; mais on obtient des résultats plus simples en employant les trois racines.

Soient θ_0, θ_1, θ_2 les trois racines de l'équation (5), on aura

$$(6)\quad \left\{\begin{array}{l} x_0 - x_1 + x_2 - x_3 = \sqrt{\theta_0}, \\ x_0 - x_2 + x_3 - x_1 = \sqrt{\theta_1}, \\ x_0 - x_3 + x_1 - x_2 = \sqrt{\theta_2}; \end{array}\right.$$

d'ailleurs

$$(7)\quad x_0 + x_1 + x_2 + x_3 = -p,$$

et les équations (6) et (7), qui sont du premier degré, donneront les valeurs suivantes des quatre racines :

$$(8)\quad \left\{\begin{array}{l} x_0 = \dfrac{-p + \sqrt{\theta_0} + \sqrt{\theta_1} + \sqrt{\theta_2}}{4}, \\ x_1 = \dfrac{-p - \sqrt{\theta_0} - \sqrt{\theta_1} + \sqrt{\theta_2}}{4}, \\ x_2 = \dfrac{-p + \sqrt{\theta_0} - \sqrt{\theta_1} - \sqrt{\theta_2}}{4}, \\ x_3 = \dfrac{-p - \sqrt{\theta_0} + \sqrt{\theta_1} - \sqrt{\theta_2}}{4}. \end{array}\right.$$

Telle est l'expression de la racine de la résolvante en t. C'est une fonction linéaire des racines de la proposée, qui peut prendre effectivement six valeurs égales deux à deux et de signes contraires, par les substitutions des racines x_0, x_1, x_2, x_3.

515. MÉTHODE DE LAGRANGE. — D'après la théorie générale que nous avons exposée aux nos 501 et 502, on peut exprimer rationnellement les quatre racines de l'équation du quatrième degré par une fonction de ces racines telle, que les 1.2.3.4 valeurs qu'on en déduit par les substitutions soient différentes. Une pareille fonction dépend d'une équation du vingt-quatrième degré; mais nous venons de voir, par l'analyse de la méthode de Ferrari, qu'il suffit, pour résoudre l'équation du quatrième degré, de connaître une fonction des racines qui ait seulement trois valeurs distinctes, ou six valeurs égales deux à deux et de signes contraires.

La formation directe de l'équation dont dépend une pareille fonction des racines de la proposée et la détermination subséquente de ses racines constituent une nouvelle méthode due à Lagrange, et que nous allons actuellement développer.

Soit l'équation

$$(1) \qquad x^4 + px^3 + qx^2 + rx + s = 0,$$

et désignons par x_0, x_1, x_2, x_3 ses quatre racines. La fonction la plus simple de ces racines, parmi celles qui ne peuvent acquérir que trois valeurs, est $x_0 x_2 + x_1 x_3$; posons donc

$$y = x_0 x_2 + x_1 x_3$$

et commençons par chercher la valeur de y, ou plutôt l'équation du troisième degré dont dépend cette quantité.

517. La discussion des cas particuliers de l'équation du quatrième degré n'offre aucune difficulté. Les formules (6) ou (8) donnent immédiatement les résultats suivants.

1° Si la réduite a deux racines égales différentes de zéro, la proposée a deux racines égales; les deux autres racines sont différentes de celles-ci, et différentes entre elles.

2° Si la réduite a deux racines nulles, la proposée a deux couples de racines égales.

3° Si les trois racines de la réduite sont égales entre elles et différentes de zéro, la proposée a trois racines égales.

4° Si la réduite a trois racines nulles, les quatre racines de la proposée sont égales entre elles.

Lorsque les coefficients p, q, r, s sont réels, la nature des racines de la réduite fait connaître celle des racines de la proposée.

Si les trois racines de la réduite sont réelles, et qu'aucune d'elles ne soit négative, il est évident, par les formules (8), que les quatre racines de la proposée sont réelles; si au contraire la réduite a une ou deux racines négatives, les quatre racines de la proposée sont imaginaires : toutefois deux de ces racines deviennent réelles et égales lorsque la réduite a deux racines négatives égales entre elles. Le dernier terme de la réduite (5) n'étant jamais positif, cette réduite ne peut avoir une seule racine négative que dans le cas où elle a une racine nulle. Si la réduite a deux racines imaginaires, on peut supposer que, dans les formules (8), $\sqrt{\theta_0}$ et $\sqrt{\theta_1}$ soient des imaginaires conjuguées, et que $\sqrt{\theta_2}$ soit réelle; on voit alors que la proposée a deux racines réelles et deux racines imaginaires.

degré

$$(4) \qquad z^2 - y_0 z + s = 0.$$

Soient z_0 et z_1 les racines de cette équation (4), on aura

$$x_0 x_2 = z_0, \quad x_1 x_3 = z_1;$$

connaissant ainsi les valeurs des fonctions $x_0 x_2$ et $x_1 x_3$, on voit de suite qu'on doit en déduire rationnellement les sommes $x_0 + x_2$ et $x_1 + x_3$, qui sont des fonctions respectivement semblables à $x_0 x_2$ et $x_1 x_3$. On a effectivement

$$x_1 x_3 (x_0 + x_2) + x_0 x_2 (x_1 + x_3) = -r,$$

ou

$$z_1 (x_0 + x_2) + z_0 (x_1 + x_3) = -r;$$

d'ailleurs

$$(x_0 + x_2) + (x_1 + x_3) = -p,$$

donc

$$x_0 + x_2 = \frac{r - pz_1}{z_1 - z_0}, \quad x_1 + x_3 = \frac{pz_0 - r}{z_1 - z_0}.$$

Connaissant $x_0 + x_2$ et $x_0 x_2$, $x_1 + x_3$ et $x_1 x_3$, on peut former deux équations du deuxième degré, ayant pour racines, la première x_0 et x_2, la seconde x_1 et x_3, et le problème peut être regardé comme résolu.

516. On résout plus facilement l'équation du quatrième degré, en prenant une résolvante dont la racine soit une fonction linéaire des racines de l'équation proposée, ayant six valeurs égales deux à deux et de signes contraires.

Soit

$$t = x_0 - x_1 + x_2 - x_3;$$

cette fonction ayant six valeurs, elle dépendra d'une équation du sixième degré; mais parce que les valeurs de t sont égales deux à deux et de signes contraires, l'équation s'abaissera au troisième degré, en posant $t^2 = \theta$. On peut former directement l'équation en θ, puisqu'on

et à identifier l'équation finale en x avec la proposée dont les racines seront alors données par la formule

$$x = a + b\sqrt[4]{e} + c(\sqrt[4]{e})^2 + d(\sqrt[4]{e})^3.$$

Tout revient donc à déterminer les valeurs des indéterminées a, b, c, d, e, dont l'une peut être choisie arbitrairement.

Sur la résolution algébrique des équations.

519. Toutes les méthodes connues que les géomètres ont essayé d'appliquer à la résolution algébrique des équations, et il en serait nécessairement de même des nouvelles qu'on pourrait imaginer, reviennent à faire dépendre la résolution de l'équation proposée de celle d'une autre équation plus facile à résoudre, et dont les racines soient des fonctions de celles de la proposée.

C'est ainsi que l'équation du deuxième degré peut être résolue en déterminant la fonction $x_1 - x_0$ de ses deux racines. Le carré de cette fonction est une fonction symétrique, et, sa valeur étant connue, la résolution de l'équation en résulte par l'extraction d'une racine carrée.

C'est encore ainsi que nous avons pu résoudre l'équation du troisième degré en déterminant la valeur d'une fonction linéaire des racines x_0, x_1, x_2, savoir :

$$t = x_0 + \alpha x_1 + \alpha^2 x_2,$$

α désignant l'une des racines imaginaires de l'équation $x^3 = 1$. Le cube t^3 de cette fonction ne peut prendre que deux valeurs distinctes par les substitutions des racines x_0, x_1, x_2, et il dépend, par conséquent, d'une équation du deuxième degré.

Enfin nous avons résolu l'équation du quatrième

degré en déterminant la valeur de l'une des deux fonctions suivantes de ses racines x_0, x_1, x_2, x_3 :

$$y = x_0 x_2 + x_1 x_3,$$
$$t = x_0 - x_1 + x_2 - x_3.$$

La première de ces deux fonctions ne peut acquérir que trois valeurs, et elle dépend, par conséquent, d'une équation du troisième degré, qu'on sait résoudre ; la seconde fonction peut prendre six valeurs, et elle dépend d'une équation qui est du sixième degré, mais qui peut être abaissée au troisième, parce qu'elle ne contient que des puissances paires de l'inconnue. Nous avons vu que la résolvante en t conduit plus aisément que celle en y à la résolution de la proposée ; elle a aussi cet avantage, que la résolution de l'équation du quatrième degré, qu'on en déduit, présente la plus complète analogie avec celle de l'équation du troisième degré. La fonction t peut, en effet, s'écrire ainsi :

$$t = x_0 + \alpha x_1 + \alpha^2 x_2 + \alpha^3 x_3,$$

α désignant la racine réelle -1 de l'équation $x^4 = 1$.

Dans les *Mémoires de l'Académie de Berlin* (années 1770 et 1771) (¹), Lagrange, prenant pour point de départ les résultats qui précèdent, a cherché à opérer la résolution de l'équation de degré n dont x_0, x_1, x_2, ..., x_{n-1} sont les n racines, en employant une fonction de la forme

$$t = x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-2} x_{n-2} + \alpha^{n-1} x_{n-1},$$

où α désigne une racine de l'équation $x^n = 1$.

Quoique ces recherches de Lagrange n'aient pu le

(¹) Lagrange a donné un extrait de son Mémoire dans la Note XIII de son *Traité de la résolution des équations numériques*, 3ᵉ édition, p. 242.

conduire à la résolution des équations générales d'un degré supérieur au quatrième, problème dont l'impossibilité est aujourd'hui démontrée, les développements qu'il a donnés à ce sujet ont une importance considérable, et nous allons les présenter ici.

Nous suivrons la marche tracée par l'illustre auteur, et nous distinguerons avec lui le cas où le degré de l'équation est un nombre premier, et le cas où ce degré est un nombre composé.

Des équations dont le degré est un nombre premier.

520. Désignons par

$$x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1}$$

les n racines d'une équation

$$(1)\qquad V = 0,$$

d'un degré premier n, par α une racine quelconque de l'équation $x^n = 1$, et posons

$$(2)\qquad t = x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1}.$$

Si α n'est pas égal à 1, n étant premier, les puissances de α, savoir :

$$1,\ \alpha,\ \alpha^2,\ \ldots,\ \alpha^{n-1},$$

sont les n racines de l'équation $x^n = 1$, et par conséquent elles sont distinctes. Il résulte de là que la fonction t prendra $1.2.3\ldots n$ valeurs distinctes, par les substitutions des racines, ainsi que nous l'avons déjà dit au n° 494; cette fonction dépend donc d'une équation du degré

$$1.2.3\ldots n,$$

qu'on peut former par la méthode du n° 180, puisqu'on

connaît la composition de ses racines. Mais d'après les développements présentés au n° 494, *la résolution de cette équation de degré* $1.2.3\ldots n$ *peut être ramenée à la résolution d'une équation du degré* $n-1$, *dont les coefficients dépendent d'une équation du degré* $1.2.3\ldots(n-2)$.

En effet, si z désigne successivement tous les indices

$$0,\ 1,\ 2,\ \ldots,\ (n-1)$$

à des multiples près de n, que l'on néglige, la substitution circulaire

$$\binom{z+1}{z},$$

exécutée sur la fonction t, équivaut (n° 494) à la multiplication de t par α, et il en résulte que l'équation dont t dépend ne renferme que des termes dont les degrés sont divisibles par n; cette équation s'abaissera donc au degré $1.2.3\ldots(n-1)$, si l'on pose

$$\theta = t^n.$$

Soient

$$(3)\qquad \theta_0,\ \theta_1,\ \theta_2,\ \ldots,\ \theta_{n-2}$$

les résultats que l'on obtient en remplaçant α par chacune des racines

$$\alpha,\ \beta,\ \gamma,\ \ldots,\ \omega$$

de l'équation

$$\frac{x^n-1}{x-1}=0,$$

dans l'expression

$$(4)\qquad \theta = (x_0+\alpha x_1+\alpha^2 x_2+\ldots+\alpha^{n-1}x_{n-1})^n.$$

On a vu au n° 494 que, si r désigne une racine primitive pour le nombre premier n, les quantités (3) sont

précisément les valeurs que prend θ quand on exécute dans cette fonction les $n-2$ puissances de la substitution circulaire

$$\begin{pmatrix} rz \\ z \end{pmatrix},$$

et nous avons conclu de ce fait que toute fonction symétrique Θ des quantités (3) est invariable par les deux substitutions circulaires

$$\begin{pmatrix} z+1 \\ z \end{pmatrix}, \quad \begin{pmatrix} rz \\ z \end{pmatrix}.$$

Cela posé, une substitution quelconque peut être regardée comme le produit de trois substitutions, savoir : 1° une puissance de $\begin{pmatrix} z+1 \\ z \end{pmatrix}$; 2° une puissance de $\begin{pmatrix} rz \\ z \end{pmatrix}$ qui ne déplace pas l'indice 0 ; 3° une substitution qui ne déplace aucun des indices 0 et 1. Les deux premières de ces substitutions ne produiront aucun changement dans Θ, et, par conséquent, on obtiendra toutes les valeurs distinctes de cette fonction en exécutant les $1.2.3\ldots(n-2)$ substitutions des $n-2$ indices $2, 3, \ldots, (n-1)$. D'après cela, si l'on représente par

$$(5) \quad \theta^{n-1} + P_1\theta^{n-2} + P_2\theta^{n-3} + \ldots + P_{n-2}\theta + P_{n-1} = 0$$

l'équation qui a pour racines les $n-1$ valeurs (3) de θ, chacun des coefficients P_1, P_2, ..., dépendra d'une équation du degré $1.2.3\ldots(n-2)$, et l'on pourra former ces diverses équations par la méthode du n° 180, puisqu'on connaît la composition de leurs racines. Mais on aperçoit immédiatement que tous ces coefficients P_1, P_2, ... ne dépendent que d'une seule équation du degré $1.2.3\ldots(n-2)$, car ce sont évidemment des fonctions semblables des racines $x_0, x_1, \ldots, x_{n-1}$ de l'équation

proposée, et si l'on se donne la valeur de l'un d'eux, celles de tous les autres s'en déduiront rationnellement.

Voici comment on peut opérer pour former l'équation dont P_1 dépend, et pour exprimer en fonction de P_1 les autres coefficients P_2, P_3, ... On calculera l'équation de degré $1.2.3\ldots(n-1)$, qui a pour racines toutes les valeurs de θ et dont les coefficients, fonctions invariables des racines de la proposée, sont exprimables rationnellement par ses coefficients. Le premier membre de l'équation (5) étant un diviseur du premier membre de cette équation complète en θ, on fera la division à la manière ordinaire, et l'on égalera à zéro les $n-1$ termes du reste. Les $n-2$ premières des équations ainsi obtenues serviront à déterminer les coefficients P_2, P_3, ..., en fonction de P_1, et l'on aura ensuite l'équation en P_1 de degré $1.2.3\ldots(n-2)$, en remplaçant dans la $(n-1)^{\text{ième}}$, P_2, P_3, ... par les valeurs qu'on aura trouvées.

Lagrange a cherché à simplifier les calculs, presque impraticables dès le cinquième degré, auxquels conduit l'application de la théorie précédente ; il a effectivement imaginé un artifice ingénieux pour exprimer les coefficients de l'équation (5), en fonction des racines x_0, x_1, ... Je vais le rapporter ici.

Pour avoir l'expression de θ, il faut élever à la $n^{\text{ième}}$ puissance la quantité

$$x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1};$$

en faisant ce calcul, et ayant soin de rabaisser les exposants de α au-dessous de n, on a un résultat de la forme

$$(6)\qquad \theta = \xi_0 + \alpha\xi_1 + \alpha^2\xi_2 + \ldots + \alpha^{n-1}\xi_{n-1}.$$

La formule (6) donne les valeurs de θ_0, θ_1, ..., θ_{n-2},

quand on substitue à α chacune des racines imaginaires α, β, γ, ... ω de l'équation $x^n = 1$. En outre, si l'on remplace α par 1, le second membre de l'équation (6) a pour valeur $(x_0 + x_1 + \ldots + x_{n-1})^n$ ou A^n, en désignant par A la somme connue des racines de l'équation proposée (1). On a donc

$$\begin{aligned}
A^n &= \xi_0 + \xi_1 + \xi_2 + \ldots + \xi_{n-1},\\
\theta_0 &= \xi_0 + \alpha\xi_1 + \alpha^2\xi_2 + \ldots + \alpha^{n-1}\xi_{n-1},\\
\theta_1 &= \xi_0 + \beta\xi_1 + \beta^2\xi_2 + \ldots + \beta^{n-1}\xi_{n-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\theta_{n-2} &= \xi_0 + \omega\xi_1 + \omega^2\xi_2 + \ldots + \omega^{n-1}\xi_{n-1}.
\end{aligned}$$

Ajoutons ces équations et désignons par S_1 la somme des racines de l'équation (5); on aura, d'après les propriétés des racines α, β, ...,

$$A^n + S_1 = n\xi_0,$$

ou

$$S_1 = n\xi_0 - A^n.$$

Désignons généralement par S_ν la somme des $\nu^{\text{ièmes}}$ puissances des racines de l'équation (5); élevons l'expression (6) à la puissance ν, et rabaissant les exposants de α au-dessous de n, représentons le résultat par

$$\theta^\nu = \xi_0^{(\nu)} + \alpha\xi_1^{(\nu)} + \alpha^2\xi_2^{(\nu)} + \ldots + \alpha^{n-1}\xi_{n-1}^{(\nu)};$$

remplaçons ensuite α successivement par 1, α, β, ...ω, et ajoutons les résultats, on aura

$$A^{\nu n} + S_\nu = n\xi_0^{(\nu)},$$

ou

$$S_\nu = n\xi_0^{(\nu)} - A^{\nu n}.$$

On pourra calculer de cette manière, en fonction des racines x_0, x_1, ..., x_{n-1}, les sommes S_2, S_3, ..., S_{n-1},

et l'on en déduira ensuite les valeurs suivantes des coefficients P_1, P_2, ... de l'équation (5) :

$$P_1 = -(n\xi_0 - A^n),$$

$$P_2 = +\frac{(n\xi_0 - A^n)^2}{2} - \frac{(n\xi_0^{(2)} - A^{2n})}{2},$$

$$P_3 = -\frac{(n\xi_0 - A^n)^3}{2.3} + \frac{(n\xi_0 - A^n)(n\xi_0^{(2)} - A^{2n})}{2} - \frac{(n\xi_0^{(3)} - A^{3n})}{3},$$

....

Voilà donc les coefficients P_1, P_2, ... de l'équation (5) exprimés en fonction des racines x_0, x_1, ..., x_{n-1} de l'équation proposée, et si l'on fait dans l'expression de l'un d'eux, dans celle de P_1 par exemple, toutes ces substitutions des racines, on ne trouvera que $1.2.3\ldots(n-2)$ valeurs distinctes. On pourra ainsi former directement l'équation en P_1, et l'on exprimera ensuite les valeurs des autres coefficients en fonction rationnelle de P_1, par le procédé indiqué plus haut.

Si l'on connaît un seul système de valeurs des coefficients P_1, P_2, ..., et si l'on peut résoudre l'équation en θ correspondante de degré $n-1$, la résolution de l'équation proposée (1) s'ensuivra immédiatement, comme nous allons le faire voir.

Dans l'hypothèse où nous nous plaçons, les quantités θ_0, θ_1, ..., θ_{n-1} sont connues, et l'équation (4) donne, en mettant α, β, γ, ..., ω au lieu de α,

$$(7)\quad \left\{\begin{array}{l} x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1} = \sqrt[n]{\theta_0}, \\ x_0 + \beta x_1 + \beta^2 x_2 + \ldots + \beta^{n-1} x_{n-1} = \sqrt[n]{\theta_1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_0 + \omega x_1 + \omega^2 x_2 + \ldots + \omega^{n-1} x_{n-1} = \sqrt[n]{\theta_{n-2}}; \end{array}\right.$$

on a d'ailleurs

$$x_0 + x_1 + x_2 + \ldots + x_{n-1} = A;$$

donc, en ajoutant ces équations, et en ayant égard aux propriétés des racines α, β, ..., on aura

$$(8)\qquad x_1 = \frac{A + \sqrt[n]{\theta_0} + \sqrt[n]{\theta_1} + \ldots + \sqrt[n]{\theta_{n-2}}}{n};$$

ajoutant aussi ces mêmes équations respectivement multipliées par α^ν, β^ν, ..., ω^ν et 1, il viendra

$$(9)\qquad x_{n-\nu} = \frac{A + \alpha^\nu\sqrt[n]{\theta_0} + \beta^\nu\sqrt[n]{\theta_1} + \ldots + \omega^\nu\sqrt[n]{\theta_{n-2}}}{n}.$$

Mais, comme rien ne détermine celle des valeurs de chaque radical qu'il faut prendre, le second membre de l'équation (9) ne diffère pas du second membre de l'équation (8). Aussi doit-on se borner à dire que les n racines de l'équation proposée sont données par la formule unique

$$(10)\qquad x = \frac{A + \sqrt[n]{\theta_1} + \sqrt[n]{\theta_2} + \ldots + \sqrt[n]{\theta_{n-2}}}{n}.$$

A la vérité, cette formule, à cause de la multiplicité des valeurs de chaque radical, donne pour x un nombre de valeurs égal à n^{n-1} ; mais on peut faire disparaître l'ambiguïté qui en résulte. En effet, les premiers membres des équations (7) sont des fonctions semblables des racines $x_0, x_1, \ldots$: on pourra donc, si l'on se donne l'une de ces fonctions, en déduire rationnellement toutes les autres. Ainsi, on pourra exprimer $\sqrt[n]{\theta_1}$, $\sqrt[n]{\theta_2}$, ..., $\sqrt[n]{\theta_{n-1}}$ rationnellement en fonction de $\sqrt[n]{\theta_0}$, et la formule (10) ne donnera alors pour x que n valeurs, comme cela doit être.

Par cette méthode, la résolution de l'équation du cinquième degré se ramène à celle d'une équation du quatrième degré, dont les coefficients dépendent d'une équation du sixième.

Des équations dont le degré est un nombre composé.

521. L'analyse précédente n'est pas applicable aux équations dont le degré est un nombre composé, et il est nécessaire d'employer ici des considérations nouvelles. La méthode que Lagrange a proposée pour ce cas revient au fond à décomposer l'équation proposée

$$(1) \qquad V = 0,$$

de degré $m = np$, n étant un nombre premier, en n équations du degré p; et cette méthode n'exige pour cela que la résolution d'une équation du degré

$$\frac{1.2\ldots m}{(n-1)n(1.2\ldots p)^n},$$

et celle d'une équation du degré $n-1$, tandis que si l'on cherchait à faire la décomposition par la méthode ordinaire, il faudrait résoudre une équation du degré

$$\frac{m(m-1)\ldots(m-p+1)}{1.2\ldots p}.$$

Cette décomposition de l'équation (1) en n équations de degré p ayant été effectuée, on pourra appliquer à chacune de ces dernières la méthode exposée précédemment, si p est un nombre premier. Dans le cas contraire, si $p = n'p'$, n' étant un nombre premier, on ramènera la résolution de chaque équation de degré p à celle de n' équations du degré p', en opérant de la même manière que pour la proposée; et ainsi de suite. Entrons maintenant dans les détails.

Soit $m = np$, n étant un nombre premier, et posons, comme précédemment,

$$t = x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{m-1} x_{m-1},$$

$x_0, x_1, \ldots, x_{m-1}$ désignant les m racines de l'équation (1)

et α une racine de $x^m = 1$, mais qui appartienne aussi à l'équation $x^n = 1$. Alors, comme on a généralement

$$\alpha^{n+k} = \alpha^k,$$

la valeur précédente de t pourra s'écrire comme il suit:

$$\begin{aligned} t = & [x_0 + x_n + x_{2n} + \ldots + x_{(p-1)n}] \\ & + \alpha[x_1 + x_{n+1} + x_{2n+1} + \ldots + x_{(p-1)n+1}] \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & + \alpha^{n-1}[x_{n-1} + x_{2n-1} + \ldots + x_{pn-1}], \end{aligned}$$

ou

$$t = X_0 + \alpha X_1 + \alpha^2 X_2 + \ldots + \alpha^{n-1} X_{n-1},$$

en faisant, pour abréger,

$$(2) \quad \left\{ \begin{aligned} X_0 &= x_0 + x_n + x_{2n} + \ldots + x_{(p-1)n}, \\ X_1 &= x_1 + x_{n+1} + x_{2n+1} + \ldots + x_{(p-1)n+1}, \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ X_{n-1} &= x_{n-1} + x_{2n-1} + x_{3n-1} + \ldots + x_{pn-1}. \end{aligned} \right.$$

Représentons par

$$(3) \qquad W = 0$$

l'équation qui a pour racines $X_0, X_1, \ldots X_{n-1}$; on pourra appliquer à cette équation (3) la méthode exposée précédemment pour les équations de degré premier. Faisons $\theta = t^n$, ou

$$(4) \qquad \theta = (X_0 + \alpha X_1 + \ldots + \alpha^{n-1} X_{n-1})^n:$$

θ dépend d'une équation du degré $1.2.3\ldots(n-1)$ dont les coefficients peuvent s'exprimer rationnellement par ceux de l'équation (3); et si l'on représente par $\theta_0, \theta_1, \ldots \theta_{n-2}$ les $n-1$ valeurs que prend θ, quand on remplace α par les $n-1$ racines imaginaires de $x^n = 1$, on pourra former l'équation de degré $n-1$ qui a ces $n-1$ valeurs de θ pour racines : représentons cette équation par

$$(5) \quad \theta^{n-1} + P_1 \theta^{n-2} + P_2 \theta^{n-3} + \ldots + P_{n-2}\theta + P_{n-1} = 0;$$

ses coefficients P_1, P_2, ... dépendent d'une seule équation de degré $1.2.3\ldots(n-2)$ dont les coefficients s'expriment rationnellement par ceux de l'équation (3), ainsi que nous l'avons établi précédemment.

Soient y l'un quelconque des coefficients P_1, P_2, ... et

$$(6) \qquad f(y) = 0$$

l'équation de degré $1.2.3\ldots(n-2)$ dont y dépend. Les coefficients de cette équation (6) sont exprimables rationnellement par ceux de l'équation (3), mais ces derniers ne sont pas connus, il n'y a que ceux de l'équation (1) qui le soient; voici comment on peut former une équation en y dont les coefficients soient exprimés par les quantités connues.

$f(y)$ est une fonction de y qui contient symétriquement les quantités X_0, X_1, ..., X_{n-1}, et, si l'on y remplace X_0, X_1, ... par leurs valeurs tirées des équations (2), elle deviendra une fonction entière non symétrique des racines x_0, x_1, ..., x_{m-1} de l'équation (1). Effectuons dans $f(y)$ toutes les substitutions des racines x_0, x_1, ..., x_{m-1}, et désignons par

$$f_0(y), \quad f_1(y), \quad \ldots, \quad f_{\mu-1}(y)$$

les μ valeurs distinctes que prend ainsi $f(y)$; le produit de toutes ces valeurs est une fonction symétrique des racines x_0, x_1, ..., x_{m-1}, exprimable rationnellement par les coefficients de l'équation proposée. On a donc, pour déterminer y, l'équation

$$(7) \qquad f_0(y)f_1(y)f_2(y)\ldots f_{\mu-1}(y) = 0,$$

dont les coefficients peuvent être considérés comme connus.

Le degré de cette équation (7) est $1.2.3\ldots(n-2)\times\mu$, μ désignant le nombre des valeurs distinctes que prend

$f(y)$ par les substitutions des racines $x_0, x_1, \ldots, x_{m-1}$; nous savons que ce nombre μ est un diviseur du produit $1.2.3\ldots m$, et si l'on fait

$$\mu = \frac{1.2.3\ldots m}{\nu},$$

ν sera le nombre des substitutions qui appartiennent à la fonction $f(y)$. Or $f(y)$ ne change pas quand on change, les unes dans les autres, les racines qui figurent dans l'une des expressions $X_0, X_1, \ldots, X_{n-1}$, non plus qu'en échangeant les quantités $X_0, X_1, \ldots$, les unes dans les autres; mais toute substitution qui fait passer quelques-unes des racines contenues dans X_1, ou X_2, ou ..., dans l'une des autres fonctions, change évidemment la fonction $f(y)$. On conclut aisément de là que

$$\nu = (1.2.3\ldots p)^n (1.2\ldots n),$$

et, par conséquent,

$$\mu = \frac{1.2.3\ldots m}{(1.2.3\ldots n)(1.2.3\ldots p)^n}.$$

Le degré de l'équation (7) est donc

$$1.2.3\ldots(n-2)\frac{1.2.3\ldots m}{(1.2.3\ldots n)(1.2\ldots p)^n},$$

ou

$$\frac{1.2.3\ldots m}{(n-1)n(1.2.3\ldots p)^n},$$

ce qui s'accorde avec la proposition établie au n° 439 (corollaire II).

Si l'on connaît une seule racine de l'équation (7), on aura un système de valeurs des coefficients

$$P_1,\ P_2,\ \ldots,\ P_{n-1}$$

de l'équation (5), car ces coefficients sont des fonctions semblables des racines de l'équation proposée, et, par

conséquent, ils peuvent s'exprimer rationnellement en fonction de l'un quelconque d'entre eux et des quantités connues.

On résoudra ensuite l'équation (5), qui n'est que du degré $n-1$, et l'on aura alors aisément les racines de l'équation (3). Désignons, en effet, par

$$\theta_0,\ \theta_1,\ \theta_2,\ \ldots,\ \theta_{n-2}$$

les $n-1$ racines de l'équation (5); ces valeurs de θ étant précisément celles qu'on déduit de l'équation (4), en remplaçant α par chacune des racines imaginaires de $x^n = 1$, on aura

$$\begin{aligned}
&X_1 + \alpha X_2 + \alpha^2 X_3 + \ldots + \alpha^{n-1} X_n = \sqrt[n]{\theta_0},\\
&X_1 + \beta X_2 + \beta^2 X_3 + \ldots + \beta^{n-1} X_n = \sqrt[n]{\theta_1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&X_1 + \omega X_2 + \omega^2 X_3 + \ldots + \omega^{n-1} X_n = \sqrt[n]{\theta_{n-2}}.
\end{aligned}$$

D'ailleurs, la somme des racines $X_1, X_2, \ldots, X_n$ est connue, car elle est la même que celles des racines x_0, $x_1, \ldots, x_{m-1}$; en désignant donc par A cette somme, on aura

$$X_0 + X_1 + X_2 + \ldots + X_{n-1} = A.$$

Des équations qui précèdent, on tire cette expression générale des racines $X_0, X_1, \ldots,$

$$X = \frac{A + \sqrt[n]{\theta_0} + \sqrt[n]{\theta_1} + \ldots + \sqrt[n]{\theta_{n-2}}}{n}.$$

Il ne reste plus, maintenant, qu'à trouver les racines $x_0, x_1, \ldots$ elles-mêmes; pour cela, on considérera l'équation qui a pour racines celles de la proposée dont la somme est X_0 ou X_1, ou $\ldots$, X_0 par exemple : soit

$$x^p - X_0 x^{p-1} + Q_2 x^{p-2} + \ldots + Q_{p-1} x + Q_p = 0$$

cette équation, dont le premier membre est un diviseur

du premier membre V de la proposée. On fera la division à la manière ordinaire et l'on égalera à zéro les p termes du reste; on aura ainsi p équations dont les $p-1$ premières détermineront $Q_2, Q_3, \ldots$, en fonction de X_0, la dernière étant alors satisfaite d'elle-même. Il est évident que $Q_2, Q_3, \ldots$ doivent s'exprimer rationnellement en fonction de X_0, puisque toutes ces fonctions sont semblables. On aura donc enfin, par ce moyen, les n équations de degré p dans lesquelles peut se décomposer l'équation proposée.

Tel est le point où les travaux de Lagrange ont ramené la question de la résolution algébrique des équations. La fonction résolvante nous a donné la résolution des équations du troisième et du quatrième degré; mais elle n'est d'aucune utilité pour les équations générales de degré supérieur au quatrième, dont, au surplus, la résolution est aujourd'hui démontrée impossible. Toutefois on verra plus loin que la considération de cette fonction résolvante conduit à la résolution algébrique d'une classe fort étendue d'équations de degrés quelconques.

A la même époque où Lagrange publiait, à Berlin, le Mémoire dont nous venons de présenter les résultats principaux, Vandermonde s'occupait de la même question et présentait à l'Académie des Sciences de Paris un beau Mémoire où, par des considérations différentes de celles de Lagrange, il arrivait pourtant aux mêmes conséquences. Je me borne ici à indiquer ce travail de Vandermonde, imprimé dans les *Mémoires de l'Académie des Sciences de Paris* (année 1771).

CHAPITRE II.

DE L'IMPOSSIBILITÉ DE LA RÉSOLUTION ALGÉBRIQUE DES ÉQUATIONS GÉNÉRALES AU DELA DU QUATRIÈME DEGRÉ.

Des fonctions algébriques.

522. Les considérations que nous avons développées dans le Chapitre précédent donnent lieu de penser qu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième. Abel est parvenu à démontrer rigoureusement cette impossibilité par une méthode qui a été simplifiée ensuite par Wantzel dans quelques-unes de ses parties.

Résoudre une équation algébriquement, c'est former une fonction algébrique des coefficients qui, substituée à l'inconnue, satisfasse identiquement à l'équation; la première chose à faire, pour reconnaître si une équation est soluble ou non algébriquement, est donc d'étudier la forme générale des fonctions algébriques. C'est cette étude que nous allons faire ici, et nous en conclurons ensuite facilement l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Soient

$$x_1,\ x_2,\ x_3,\ \ldots,\ x_k$$

k quantités quelconques indépendantes, et v une fonction de ces quantités; v sera une *fonction algébrique*, si on peut l'exprimer en x_1, x_2, x_3, ..., par le moyen des opérations suivantes, effectuées un nombre fini de

fois : 1° l'addition ou la soustraction; 2° la multiplication; 3° la division; 4° l'extraction des racines d'indices premiers. Nous ne comptons pas l'élévation aux puissances entières et l'extraction des racines de degrés composés, parce que ces opérations sont évidemment comprises dans les quatre que nous avons mentionnées.

Des fonctions entières.

523. Lorsque la fonction v peut se former par les deux premières des quatre opérations mentionnées ci-dessus, elle est dite rationnelle et entière ou simplement entière.

Désignons par

$$f(x_1, x_2, x_3, \ldots)$$

une fonction qui peut être exprimée par une somme d'un nombre limité de termes de la forme

$$\mathrm{A} x_1^{m_1} x_2^{m_2} \ldots,$$

A désignant une constante, et m_1, m_2, ... étant des exposants entiers et positifs. L'opération désignée par f fournit une fonction entière, conformément à la définition précédente; et l'on peut généralement considérer toutes les fonctions entières comme obtenues en répétant cette opération un nombre limité de fois. Soient v_1, v_2, ... plusieurs fonctions de x_1, x_2, ..., de la même forme que f, la fonction

$$f(v_1, v_2, \ldots)$$

sera évidemment de la même forme. D'ailleurs $f(v_1, v_2, \ldots)$ est l'expression des fonctions obtenues en répétant deux fois l'opération $f(x_1, x_2, \ldots)$; d'où il suit qu'on trouvera toujours un résultat de même forme en répétant

cette même opération autant de fois que l'on voudra, et que toute fonction entière de x_1, x_2, ... peut être exprimée par une somme de termes de la forme

$$Ax_1^{m_1} x_2^{m_2} \ldots .$$

Des fonctions rationnelles.

524. Une fonction φ des quantités x_1, x_2, x_3, ... est dite rationnelle lorsqu'elle peut être exprimée par les trois premières des quatre opérations algébriques ci-dessus désignées.

Soient

$$f(x_1, x_2, x_3, \ldots), \quad F(x_1, x_2, x_3, \ldots)$$

deux fonctions entières, le quotient de ces fonctions

$$\frac{f(x_1, x_2, \ldots)}{F(x_1, x_2, \ldots)}$$

sera évidemment un cas particulier des fonctions rationnelles non entières, et l'on peut considérer toute fonction rationnelle comme obtenue en répétant plusieurs fois l'opération précédente; mais, en désignant par φ_1, φ_2, ... plusieurs fonctions de la forme $\frac{f(x_1, x_2, \ldots)}{F(x_1, x_2, \ldots)}$, il est évident que la fonction

$$\frac{f(\varphi_1, \varphi_2, \ldots)}{F(\varphi_1, \varphi_2, \ldots)}$$

peut être réduite à la même forme; d'où il suit que toute fonction rationnelle se réduira à la forme

$$\frac{f(x_1, x_2, \ldots)}{F(x_1, x_2, \ldots)},$$

f et F désignant des fonctions entières.

Classification des fonctions algébriques non rationnelles.

525. Soit

$$f(x_1, x_2, \ldots)$$

une fonction rationnelle quelconque; il est évident que toute fonction algébrique s'obtiendra en combinant l'opération désignée par f avec l'opération désignée par $\sqrt[m]{\ }$, m étant un nombre premier. Si donc p_1, p_2, ... désignent des fonctions rationnelles de x_1, x_2, ..., n_1, n_2, ... des nombres premiers, et qu'on fasse

$$p' = f(x_1, x_2, \ldots, \sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots),$$

p' sera la forme des fonctions algébriques dans lesquelles l'opération désignée par $\sqrt[m]{\ }$ ne porte que sur des fonctions rationnelles. Nous appellerons, avec Abel, *fonctions algébriques du premier ordre* les fonctions de la forme p'.

Soient p'_1, p'_2, ... des fonctions algébriques du premier ordre, n'_1, n'_2, ... des nombres premiers; et posons

$$p'' = f(x_1, x_2, \ldots, \sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots, \sqrt[n'_1]{p'_1}, \sqrt[n'_2]{p'_2}, \ldots),$$

p'' sera la forme générale des fonctions algébriques dans lesquelles l'opération désignée par $\sqrt[m]{\ }$ ne porte que sur des fonctions rationnelles ou sur des fonctions algébriques du premier ordre. Nous appellerons *fonctions algébriques du deuxième ordre* les fonctions de la forme p''.

De même, si p''_1, p''_2, ... désignent des fonctions algébriques du deuxième ordre, n''_1, n''_2, ... des nombres premiers, et qu'on fasse

$$p''' = f(x_1, x_2, \ldots, \sqrt[n_1]{p_1}, \ldots, \sqrt[n'_1]{p'_1}, \ldots, \sqrt[n''_1]{p''_1}, \ldots),$$

p''' sera la forme des fonctions algébriques, où l'opération désignée par $\sqrt[m]{}$ ne porte que sur des fonctions rationnelles et sur des fonctions des deux premiers ordres. Les fonctions de la forme p''' seront les fonctions algébriques du troisième ordre.

En continuant ainsi, on formera des fonctions algébriques du quatrième, cinquième, ..., $\mu^{\text{ième}}$ ordre, et il est évident que l'expression générale des fonctions du $\mu^{\text{ième}}$ ordre sera l'expression générale des fonctions algébriques.

Il suit de là qu'en désignant par v une fonction algébrique du $\mu^{\text{ième}}$ ordre, v aura la forme

$$v = f(r_1, r_2, \ldots, \sqrt[n_1]{p_1}, \sqrt[n_2]{p_2}, \ldots),$$

où f désigne toujours une fonction rationnelle, p_1, p_2, ... des fonctions de l'ordre $\mu - 1$, n_1, n_2, ... des nombres premiers, et r_1, r_2, ... des fonctions de l'ordre $\mu - 1$ ou d'un ordre moins élevé.

On peut évidemment supposer qu'aucun des radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, ... ne soit exprimable rationnellement en fonction des autres radicaux et des quantités r_1, r_2, ... Si, en effet, $\sqrt[n_1]{p_1}$ était dans ce cas, en portant sa valeur dans l'expression de v, on aurait une valeur de v

$$v = f(r_1, r_2, \ldots, \sqrt[n_2]{p_2}, \ldots),$$

de la même forme que la précédente, mais plus simple, puisqu'elle contiendrait le radical $\sqrt[n_1]{p_1}$ de moins. Si, de même, l'un des radicaux qui restent pouvait s'exprimer en fonction rationnelle des autres radicaux et des quantités r_1, r_2, ..., on pourrait chasser ce radical de l'expression de v, qui conserverait d'ailleurs la même forme; et si l'on pouvait continuer ainsi jusqu'à ce qu'on eût

éliminé tous les radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, ..., la fonction v serait réduite à l'ordre $\mu - 1$.

Si donc la fonction v est effectivement du $\mu^{\text{ième}}$ ordre, on peut supposer que les radicaux $\sqrt[n_1]{p_1}$, $\sqrt[n_2]{p_2}$, ... aient été réduits au plus petit nombre possible, et qu'il soit impossible d'exprimer l'un de ces radicaux en fonction rationnelle des autres et de fonctions algébriques d'ordre inférieur. Et si m désigne alors le nombre de ces radicaux qui affectent des fonctions algébriques d'ordre $\mu - 1$, nous dirons que la fonction v d'ordre μ est du *degré m*.

D'après cette définition, une fonction d'ordre μ et de degré zéro n'est autre qu'une fonction d'ordre $\mu - 1$, et une fonction d'ordre zéro est une fonction rationnelle.

Il résulte de là que, si v désigne une fonction algébrique d'ordre μ et de degré m, on aura généralement

$$v = f(r_1, r_2, \ldots, \sqrt[n]{p}),$$

f désignant une fonction rationnelle, p une fonction algébrique d'ordre $\mu - 1$, n un nombre premier, et r_1, r_2, ... des fonctions d'ordre μ, mais de degré $m - 1$. En outre, d'après ce qui précède, on peut toujours supposer qu'il soit impossible d'exprimer $\sqrt[n]{p}$ en fonction rationnelle de r_1, r_2, ...

Forme générale des fonctions algébriques.

526. Dans l'expression précédente de v, f désigne une fonction rationnelle des quantités r_1, r_2, ... et $\sqrt[n]{p}$, mais toute fonction rationnelle de plusieurs quantités peut être représentée par le quotient de deux fonctions entières; nous pouvons donc poser

$$v = \frac{\varphi(r_1, r_2, \ldots, \sqrt[n]{p})}{\psi(r_1, r_2, \ldots, \sqrt[n]{p})},$$

φ et ψ désignant des fonctions entières, et si l'on ordonne φ et ψ par rapport aux puissances de $\sqrt[n]{p}$ ou $p^{\frac{1}{n}}$, on aura pour v une valeur de la forme

$$v = \frac{s_0 + s_1 p^{\frac{1}{n}} + s_2 p^{\frac{2}{n}} + \ldots + s_\nu p^{\frac{\nu}{n}}}{t_0 + t_1 p^{\frac{1}{n}} + t_2 p^{\frac{2}{n}} + \ldots + t_{\nu'} p^{\frac{\nu'}{n}}} = \frac{S}{T},$$

où $s_0, s_1, \ldots, s_\nu$ et $t_0, t_1, \ldots, t_{\nu'}$ sont des fonctions entières de $r_1, r_2, \ldots$.

Soit α une racine imaginaire de l'équation

$$\alpha^n = 1;$$

désignons par

$$T_1, T_2, \ldots, T_{n-1}$$

les $n - 1$ valeurs qu'on obtient en remplaçant, dans T, $p^{\frac{1}{n}}$ successivement par

$$\alpha p^{\frac{1}{n}}, \quad \alpha^2 p^{\frac{1}{n}}, \quad \alpha^3 p^{\frac{1}{n}}, \quad \ldots, \quad \alpha^{n-1} p^{\frac{1}{n}},$$

et multiplions par $T_1 T_2 \ldots T_{n-1}$ les deux termes de la valeur de v, on aura

$$v = \frac{ST_1 T_2 \ldots T_{n-1}}{TT_1 T_2 \ldots T_{n-1}}.$$

Le produit $TT_1 T_2 \ldots T_{n-1}$ peut évidemment s'exprimer en fonction entière de p et des quantités $r_1, r_2, \ldots$; il est donc une fonction algébrique d'ordre μ et de degré $m - 1$ au plus, que nous désignerons par u. Pareillement, le produit $ST_1 T_2 \ldots T_{n-1}$ est une fonction entière de $r_1, r_2 \ldots$, et $\sqrt[n]{p}$; nous représenterons sa valeur par

$$u_0 + u_1 p^{\frac{1}{n}} + u_2 p^{\frac{2}{n}} + \ldots + u_i p^{\frac{i}{n}},$$

et l'on aura

$$v = \frac{u_0 + u_1 p^{\frac{1}{n}} + u_2 p^{\frac{2}{n}} + \ldots + u_i p^{\frac{i}{n}}}{u},$$

ou simplement

$$v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_i p^{\frac{i}{n}},$$

en mettant $q_0, q_1, \ldots$ au lieu de $\frac{u_0}{u}, \frac{u_1}{u}, \ldots$; $q_0, q_1, \ldots$ désignent ici des fonctions rationnelles de $r_1, r_2, \ldots$ et p.

On peut chasser de l'expression précédente de v les puissances de $p^{\frac{1}{n}}$ supérieures à la $(n-1)^{\text{ième}}$. Si, en effet, j désigne un nombre qui, divisé par n, donne le quotient g et le reste h, on a

$$p^{\frac{j}{n}} = p^g . p^{\frac{h}{n}},$$

et, en se servant de cette formule, on pourra mettre v sous la forme

$$(1) \qquad v = q_0 + q_1 p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

$q_0, q_1, q_2, \ldots, q_{n-1}$ étant toujours des fonctions rationnelles de $p, r_1, r_2, \ldots$, et, par conséquent, des fonctions algébriques d'ordre μ et de degré $m-1$ au plus, telles, en outre, qu'il soit impossible d'exprimer rationnellement $p^{\frac{1}{n}}$ en fonction rationnelle des quantités dont elles dépendent.

Dans l'expression (1) de v, on peut supposer

$$q_1 = 1.$$

Pour le démontrer, supposons d'abord que q_1 ne soit pas nul, et posons

$$p_1 = pq_1^n,$$

d'où

$$p = \frac{p_1}{q_1^n} \quad \text{et} \quad p^{\frac{1}{n}} = \frac{p_1^{\frac{1}{n}}}{q_1};$$

l'expression de ν devient

$$\nu = q_0 + p^{\frac{1}{n}} + \frac{q_2}{q_1^2} p^{\frac{2}{n}} + \ldots + \frac{q_{n-1}}{q_1^{n-1}} p^{\frac{n-1}{n}},$$

ou plus simplement

$$(2) \qquad \nu = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

en écrivant p au lieu de p_1; q_2, q_3, ... au lieu de $\frac{q_2}{q_1^2}$, $\frac{q_3}{q_1^3}$, ...

Dans cette nouvelle expression (2) de ν, qui se déduit de (1) en faisant $q_1 = 1$, les quantités q_0, q_2, ... désignent toujours des fonctions algébriques d'ordre μ et de degré $m - 1$.

Supposons maintenant que dans l'expression (1) de ν on ait $q_1 = 0$; désignons par q_k l'une des quantités q_2, q_3, ..., qui n'est pas nulle, et posons

$$p_1 = q_k^n p^k,$$

d'où

$$p_1^{\frac{\alpha}{n}} = q_k^\alpha p^{\frac{k\alpha}{n}},$$

n étant premier et k étant moindre que n, on peut toujours trouver deux entiers α et β tels, que

$$k\alpha - n\beta = \lambda,$$

λ étant un nombre entier quelconque donné; alors on aura

$$p_1^{\frac{\alpha}{n}} = q_k^\alpha p^\beta p^{\frac{\lambda}{n}},$$

d'où

$$p^{\frac{\lambda}{n}} = q_k^{-\alpha} p^{-\beta} p_1^{\frac{\alpha}{n}}.$$

On a, en particulier et par hypothèse,

$$p^{\frac{k}{n}} = \frac{p_1^{\frac{1}{n}}}{q_k};$$

les deux formules précédentes permettent de substituer aux puissances de $p^{\frac{1}{n}}$, dans la valeur (1) de v, celles de $p_1^{\frac{1}{n}}$, et, après cette substitution, il est évident que la forme de v n'aura pas changé, mais que le coefficient de $p_1^{\frac{1}{n}}$ sera l'unité; car, dans l'expression primitive de v, $p^{\frac{k}{n}}$ a pour coefficient q_k. Les développements qui précèdent peuvent être résumés par la proposition suivante :

Théorème. — *Toute fonction algébrique d'ordre μ et de degré m peut être mise sous la forme*

$$v = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}},$$

où n est un nombre premier, q_0, q_2, ... des fonctions algébriques d'ordre μ, mais de degré $m-1$, et p une fonction d'ordre $\mu - 1$, dont la racine $n^{\text{ième}}$ ne peut être exprimée rationnellement par les quantités q_0, q_2, ...

Propriétés des fonctions algébriques qui satisfont à une équation donnée.

527. Il importe de rappeler ici les définitions que nous avons présentées au n° 100.

Si l'on considère un polynôme entier et rationnel

$$x^m + a_1 x^{m-1} + a_2 x^{m-2} \ldots,$$

dont les coefficients $a_1, a_2, \ldots$ soient des nombres commensurables donnés, tout diviseur de ce polynôme dont les coefficients sont commensurables est dit un *diviseur commensurable*.

Plus généralement, si les coefficients $a_1, a_2, \ldots$ du polynôme sont des fonctions rationnelles de quantités quelconques, qu'on regarde comme connues, tout diviseur de ce polynôme qui a pour coefficients des fonctions rationnelles des quantités connues est appelé un *diviseur commensurable*.

On nomme, dans tous les cas, *équation irréductible* toute équation dont le premier membre n'admet aucun diviseur commensurable.

Dans le cas de l'équation générale de degré quelconque, dont les coefficients sont indéterminés, les quantités connues ne sont autres que les coefficients eux-mêmes; l'équation est nécessairement irréductible.

Cela posé, soit une équation de degré m

$$(1) \qquad x^m + a_1 x^{m-1} + a_2 x^{m-2} + \ldots + a_{m-1} x + a_m = 0,$$

dont les coefficients sont considérés comme des fonctions rationnelles de quantités connues, et supposons qu'elle soit résoluble algébriquement.

D'après la classification des fonctions algébriques établie précédemment, si la racine x est une fonction algébrique d'ordre μ des quantités connues, on pourra poser

$$(2) \qquad x = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots + q_{n-1} p^{\frac{n-1}{n}}$$

n est un nombre premier; p désigne une fonction d'ordre $- 1$; $q_0, q_2, \ldots$ peuvent être de l'ordre μ, mais sont d'un degré moindre que celui de x. Enfin on peut sup-

poser qu'il soit impossible d'exprimer $p^{\frac{1}{n}}$ en fonction rationnelle de p, q_0, q_2, ...

En substituant cette expression (2) de x dans l'équation (1), on aura un résultat qui pourra évidemment se réduire à la forme

$$(3) \qquad r_0 + r_1 p^{\frac{1}{n}} + r_2 p^{\frac{2}{n}} + \ldots + r_{n-1} p^{\frac{n-1}{n}} = 0,$$

où $r_0, r_1, r_2, \ldots, r_{n-1}$ désignent des fonctions rationnelles des quantités $p, q_0, q_2, \ldots, q_{n-1}$. Or je dis que l'équation (3) exige que l'on ait en même temps

$$r_0 = 0, \quad r_1 = 0, \quad r_2 = 0, \quad \ldots, \quad r_{n-1} = 0.$$

En effet, dans le cas contraire, les deux équations

$$z^n - p = 0,$$
$$r_0 + r_1 z + r_2 z^2 + \ldots + r_{n-1} z^{n-1} = 0$$

auraient une ou plusieurs racines communes. Soit k le nombre de ces racines, on pourrait former une équation de degré k ayant pour racines ces k racines communes, et pour coefficients des fonctions rationnelles de $p, q_0, q_2, \ldots, q_{n-1}$. Soit

$$s_0 + s_1 z + s_2 z^2 + \ldots + s_k z^k = 0$$

cette équation, et désignons par

$$t_0 + t_1 z + t_2 z^2 + \ldots + t_i z^i$$

un diviseur irréductible de son premier membre, dont les coefficients $t_0, t_1, \ldots, t_i$ soient des fonctions rationnelles de $p, q_0, q_2, \ldots, q_{n-1}$. L'équation

$$(4) \qquad t_0 + t_1 z + t_2 z^2 + \ldots + t_i z^i = 0$$

a toutes ses racines communes avec

$$(5)\qquad z^n - p = 0;$$

d'ailleurs son degré i est au moins égal à 2, car, autrement, on pourrait exprimer z ou $p^{\frac{1}{n}}$ en fonction rationnelle de $p, q_0, q_2, \ldots, q_{n-1}$. Si donc z désigne une racine quelconque de l'équation (4), cette équation aura au moins une autre racine de la forme αz, α étant une racine de l'équation

$$\alpha^n = 1;$$

l'équation (4) aura donc une racine commune avec

$$(6)\qquad t_0 + t_1 \alpha z + t_2 \alpha^2 z^2 + \ldots + t_i \alpha^i z^i = 0,$$

et, par conséquent, avec l'équation

$$(7)\quad (1 - \alpha^i) t_0 + (\alpha - \alpha^i) t_1 z + \ldots + (\alpha^{i-1} - \alpha^i) t_{i-1} z^{i-1} = 0,$$

que l'on obtient en retranchant de l'équation (6) l'équation (4) multipliée par α^i. Mais l'équation (4) est supposée irréductible : il est donc impossible qu'elle ait une racine commune avec l'équation (7), qui est d'un degré inférieur au sien : d'où il suit qu'on a nécessairement

$$r_0 = 0, \quad r_1 = 0, \quad \ldots, \quad r_{n-1} = 0.$$

Les équations précédentes ayant lieu, l'expression (2) de x satisfera encore à la proposée (1), quand on y aura substitué à $p^{\frac{1}{n}}$ chacune des n valeurs

$$p^{\frac{1}{n}}, \quad \alpha p^{\frac{1}{n}}, \quad 6 p^{\frac{1}{n}}, \quad \ldots, \quad \omega p^{\frac{1}{n}},$$

où 1, α, 6, ..., ω désignent les racines $n^{\text{ièmes}}$ de l'unité. On aura ainsi n racines de l'équation (1), que nous représenterons par

$$x_1, \ x_2, \ \ldots, \ x_n,$$

et dont les valeurs seront

$$(8)\quad \begin{cases} x_1 = q_0 + p^{\frac{1}{n}} + q_2 p^{\frac{2}{n}} + \ldots\ldots + q_{n-1} p^{\frac{n-1}{n}}, \\ x_2 = q_0 + \alpha p^{\frac{1}{n}} + \alpha^2 q_2 p^{\frac{2}{n}} + \ldots + \alpha^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\ x_3 = q_0 + 6 p^{\frac{1}{n}} + 6^2 q_2 p^{\frac{2}{n}} + \ldots + 6^{n-1} q_{n-1} p^{\frac{n-1}{n}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_n = q_0 + \omega p^{\frac{1}{n}} + \omega^2 q_2 p^{\frac{2}{n}} + \ldots + \omega^{n-1} q_{n-1} p^{\frac{n-1}{n}}. \end{cases}$$

On voit que ces racines sont différentes, car, si deux d'entre elles étaient égales, il résulterait de cette égalité une équation qui aurait la même forme que l'équation (3), ce qui conduit, comme nous l'avons vu, à un résultat contradictoire. Au surplus, cette remarque n'est pas indispensable pour ce qui va suivre.

En ajoutant les équations (8), en les ajoutant ensuite après les avoir respectivement multipliées par

$$1,\ \alpha^{n-1},\ 6^{n-1},\ \ldots,\ \omega^{n-1},$$

puis par

$$1,\ \alpha^{n-2},\ 6^{n-2},\ \ldots,\ \omega^{n-2},$$

puis, etc., on obtient les suivantes :

$$\begin{aligned} q_0 &= \frac{1}{n}(x_1 + x_2 + x_3 + \ldots\ldots + x_n), \\ p^{\frac{1}{n}} &= \frac{1}{n}(x_1 + \alpha^{n-1} x_2 + \ldots + \omega^{n-1} x_n), \\ q_2 p^{\frac{1}{n}} &= \frac{1}{n}(x_1 + \alpha^{n-2} x_2 + \ldots + \omega^{n-2} x_n), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ q_{n-1} p^{\frac{n-1}{n}} &= \frac{1}{n}(x_1 + \alpha x_2 + \ldots\ldots\ldots + \omega x_n). \end{aligned}$$

Il résulte de là que, si l'on regarde comme connues les

racines de l'unité, les quantités

$$p^{\frac{1}{n}},\ q_0,\ q_2,\ \ldots,\ q_{n-1}$$

sont des fonctions rationnelles des racines de l'équation (1). On a, en effet, généralement

$$q_\rho = n^{\rho-1}\,\frac{x_1+\alpha^{n-\rho}x_2+6^{n-\rho}x_3+\ldots+\omega^{n-\rho}x_n}{(x_1+\alpha^{n-1}x_2+6^{n-1}x_3+\ldots+\omega^{n-1}x_n)^\rho}.$$

Désignons maintenant par y l'une quelconque des quantités $p^{\frac{1}{n}}$, q_0, q_2, ..., q^{n-1}, et soit

(9) $$y = s_0 + v^{\frac{1}{r}} + s_2 v^{\frac{2}{r}} + \ldots + s_{r-1} v^{\frac{r-1}{r}},$$

s_0, s_2, ..., étant des fonctions qui peuvent être du même ordre que y, mais qui sont de degré inférieur. On a, par ce qui précède,

$$y = \varphi(x_1,\ x_2,\ \ldots,\ x_m),$$

φ désignant une fonction rationnelle, et x_1, x_2, ..., x_m les m racines de l'équation (1), lesquelles peuvent ne pas entrer toutes dans la fonction φ. Soit m' le nombre des valeurs que prend cette fonction φ par les substitutions des racines x_1, x_2, ...; on pourra former une équation du degré m' dont les coefficients seront exprimés rationnellement par ceux de l'équation (1), et dont les racines

$$y_1,\ y_2,\ \ldots,\ y_{m'}$$

seront les m' valeurs de la fonction φ. Et, comme la valeur (9) de y doit satisfaire à cette équation, on en conclura, comme précédemment, que les quantités

$$v,\ s_0,\ s_2,\ \ldots,\ s_{r-1}$$

sont des fonctions rationnelles de y_1, y_2, ..., $y_{m'}$, et,

par conséquent, aussi des fonctions rationnelles de x_1, $x_2, \ldots, x_m$.

Comme on peut continuer indéfiniment ce raisonnement, on conclut de ce qui précède que :

Si une équation est résoluble algébriquement, on peut donner à la racine une forme telle, que toutes les fonctions algébriques dont elle est composée soient des fonctions rationnelles des racines de l'équation proposée.

Démonstration de l'impossibilité de résoudre algébriquement les équations générales de degré supérieur au quatrième.

528. Les propriétés des racines d'une équation résoluble algébriquement, que nous venons de démontrer, ont lieu dans tous les cas, soit qu'il s'agisse d'une équation dont les coefficients ont des valeurs déterminées, soit que l'on considère ces coefficients comme indéterminés, et, par suite, les racines de l'équation comme étant des quantités quelconques, n'ayant entre elles aucune dépendance.

Nous plaçant maintenant à ce dernier point de vue, nous allons démontrer qu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième.

Ce théorème a été démontré, pour la première fois, d'une manière rigoureuse par Abel; je présenterai ici la démonstration plus simple que l'on doit à Wantzel (¹).

(¹) J'ai cru devoir reproduire le raisonnement de Wantzel; j'ai cependant supprimé quelques détails que rendent inutiles les développements dans lesquels je suis entré en traitant de la théorie des substitutions.

Soit

$$f(x) = o$$

une équation du degré m dont les coefficients sont indéterminés, et désignons par

$$x_1, x_2, \ldots, x_m$$

ses m racines, que nous supposons exprimables algébriquement en fonction des coefficients.

Si l'équation $f(x) = o$ est satisfaite par la valeur x_1 de x, quels que soient ses coefficients, on doit reproduire identiquement x_1 en substituant dans son expression la fonction rationnelle correspondant à chaque radical, puisque les racines de l'équation sont alors entièrement arbitraires. De même, toute relation entre les racines devra être identique, et ne cessera pas d'exister, si l'on y remplace ces racines les unes par les autres, d'une manière quelconque.

Désignons par y le premier radical qui entre dans la valeur de x_1, en suivant l'ordre du calcul, et soit

$$y^n = p;$$

p dépendra immédiatement des coefficients de $f(x) = o$, et s'exprimera par une fonction symétrique des racines, $F(x_1, x_2, x_3, \ldots)$; y sera une fonction rationnelle $\varphi(x_1, x_2, x_3, \ldots)$ des mêmes racines.

Comme la fonction φ n'est pas symétrique, sans quoi la racine $n^{\text{ième}}$ de p s'extrairait exactement, elle doit changer lorsqu'on transpose deux racines, x_1, x_2, par exemple; mais la relation

$$\varphi^n = F$$

sera toujours satisfaite. D'ailleurs, la fonction F étant invariable par cette transposition, les valeurs de φ sont

des racines de l'équation $y^n = F$, et l'on a

$$\varphi(x_2, x_1, x_3, \ldots) = \alpha\varphi(x_1, x_2, x_3, \ldots),$$

α étant une racine $n^{\text{ième}}$ de l'unité.

Si l'on transpose les racines x_1 et x_2, il vient

$$\varphi(x_1, x_2, x_3, \ldots) = \alpha\varphi(x_2, x_1, x_3, \ldots);$$

d'où, en multipliant par ordre,

$$\alpha^2 = 1.$$

Ce résultat prouve que le nombre n, supposé premier, est nécessairement égal à 2; *donc le premier radical qui se présente dans la valeur de l'inconnue doit être du deuxième degré*. C'est ce qui arrive, en effet, pour les équations qu'on sait résoudre.

La fonction φ n'ayant que deux valeurs, elle change par une transposition quelconque, et elle ne sera pas changée (n° 493) par une substitution circulaire de trois ou de cinq lettres, car chacune de ces substitutions équivaut à un nombre pair de transpositions.

Continuons la série des opérations indiquées pour former la valeur x_1 de x.

On combinera le premier radical avec les coefficients de $f(x) = 0$, ou la fonction φ avec des fonctions symétriques des racines, à l'aide des premières opérations de l'Algèbre, et l'on obtiendra ainsi une fonction des racines susceptible de deux valeurs, et, par conséquent, invariable par les substitutions circulaires de trois lettres. Les radicaux subséquents pourront donner encore des fonctions du même genre, s'ils sont du deuxième degré. Supposons qu'on soit arrivé à un radical pour lequel la fonction rationnelle équivalente ne soit pas invariable par ces substitutions; désignons-le toujours par

$$y = \varphi(x_1, x_2, x_3, \ldots).$$

Dans l'équation

$$y^n = p$$

nous ferons encore

$$p = \mathrm{F}(x_1,\ x_2,\ x_3,\ \ldots);$$

cette fonction ne sera pas symétrique, mais seulement invariable par les substitutions circulaires de trois lettres. Si l'on remplace

$$x_1,\ x_2,\ x_3$$

par

$$x_2,\ x_3,\ x_1$$

dans φ, la relation

$$\varphi^n = \mathrm{F}$$

subsistera toujours; et, puisque F ne change pas par cette substitution, il viendra

$$\varphi(x_2,\ x_3,\ x_1,\ x_4,\ \ldots) = \alpha\varphi(x_1,\ x_2,\ x_3,\ x_4,\ \ldots),$$

α désignant une racine $n^{\text{ième}}$ de l'unité.

En faisant dans cette équation la substitution circulaire

$$(x_1,\ x_2,\ x_3),$$

et en répétant cette substitution, on aura

$$\varphi(x_3,\ x_1,\ x_2,\ x_4,\ \ldots) = \alpha\varphi(x_2,\ x_3,\ x_1,\ x_4,\ \ldots),$$
$$\varphi(x_1,\ x_2,\ x_3,\ x_4,\ \ldots) = \alpha\varphi(x_3,\ x_1,\ x_2,\ x_4,\ \ldots),$$

puis, en multipliant les trois équations précédentes, on conclura

$$\alpha^3 = 1.$$

Ainsi, n sera égal à 3.

Si le nombre des quantités x_1, x_2, x_3, x_4, ... est supérieur à quatre, ou si l'équation $f(x) = 0$ est d'un degré plus élevé que le quatrième, on pourra effectuer

dans φ une substitution circulaire de cinq lettres, par exemple

$$(x_1, x_2, x_3, x_4, x_5);$$

la fonction F ne changera pas par cette substitution, et l'on aura

$$\varphi(x_2, x_3, x_4, x_5, x_1, \ldots) = \alpha\varphi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

puis, en répétant de part et d'autre la même substitution,

$$\varphi(x_3, x_4, x_5, x_1, x_2, \ldots) = \alpha\varphi(x_2, x_3, x_4, x_5, x_1, \ldots),$$

....

Par la multiplication, on obtient

$$\alpha^5 = 1,$$

ce qui entraîne

$$\alpha = 1,$$

puisque α est une racine cubique de l'unité. Donc, si le degré de l'équation proposée est supérieur à 4, la fonction φ est invariable par les substitutions circulaires de trois lettres, ce qui est contraire à notre hypothèse.

Ainsi, *tous les radicaux renfermés dans l'expression de la racine d'une équation générale de degré supérieur au quatrième devraient être égaux à des fonctions rationnelles des racines invariables par les substitutions circulaires de trois racines*. En substituant ces fonctions dans l'expression de x_1, on arrive alors à une égalité de la forme

$$x_1 = \psi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

qui doit être identique; or cela est impossible, puisque le second membre reste invariable quand on remplace x_1, x_2, x_3 par x_2, x_3, x_1, tandis que le premier membre change évidemment.

Donc il est impossible de résoudre par radicaux l'é-

quation générale du cinquième degré ou d'un degré supérieur.

La démonstration précédente fait voir en même temps que, pour les équations du troisième et du quatrième degré, le premier radical, dans l'ordre des opérations, doit être un radical carré, et le deuxième un radical cubique. Ces circonstances se présentent, en effet, dans les formules que nous avons données dans le Chapitre précédent.

dans φ une substitution circulaire de cinq lettres, par exemple

$$(x_1, x_2, x_3, x_4, x_5);$$

la fonction F ne changera pas par cette substitution, et l'on aura

$$\varphi(x_2, x_3, x_4, x_5, x_1, \ldots) = \alpha\varphi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

puis, en répétant de part et d'autre la même substitution,

$$\varphi(x_3, x_4, x_5, x_1, x_2, \ldots) = \alpha\varphi(x_2, x_3, x_4, x_5, x_1, \ldots),$$

....

Par la multiplication, on obtient

$$\alpha^5 = 1,$$

ce qui entraîne

$$\alpha = 1,$$

puisque α est une racine cubique de l'unité. Donc, si le degré de l'équation proposée est supérieur à 4, la fonction φ est invariable par les substitutions circulaires de trois lettres, ce qui est contraire à notre hypothèse.

Ainsi, *tous les radicaux renfermés dans l'expression de la racine d'une équation générale de degré supérieur au quatrième devraient être égaux à des fonctions rationnelles des racines invariables par les substitutions circulaires de trois racines*. En substituant ces fonctions dans l'expression de x_1, on arrive alors à une égalité de la forme

$$x_1 = \psi(x_1, x_2, x_3, x_4, x_5, \ldots),$$

qui doit être identique; or cela est impossible, puisque le second membre reste invariable quand on remplace x_1, x_2, x_3 par x_2, x_3, x_1, tandis que le premier membre change évidemment.

Donc il est impossible de résoudre par radicaux l'é-

quation générale du cinquième degré ou d'un degré supérieur.

La démonstration précédente fait voir en même temps que, pour les équations du troisième et du quatrième degré, le premier radical, dans l'ordre des opérations, doit être un radical carré, et le deuxième un radical cubique. Ces circonstances se présentent, en effet, dans les formules que nous avons données dans le Chapitre précédent.

CHAPITRE III.

DES ÉQUATIONS ABÉLIENNES.

Des équations irréductibles dont deux racines sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre.

529. Après avoir démontré qu'il est impossible de résoudre algébriquement les équations générales de degré supérieur au quatrième, il paraîtrait naturel de chercher à déterminer quelles sont les équations susceptibles d'une telle résolution. Mais, avant d'aborder ce difficile problème, il convient de présenter une étude complète d'une classe remarquable d'équations que M. Krönecker a nommées *abéliennes*.

Les équations auxquelles conduit le problème de la division du cercle en un nombre premier p de parties égales sont toujours résolubles par radicaux, et Gauss a montré, dans ses *Recherches arithmétiques*, que chacun des radicaux dont l'expression des racines est composée a pour indice l'un des facteurs premiers de $p-1$. Ces équations ont cette propriété, que chaque racine peut s'exprimer rationnellement par l'une quelconque des autres, et Abel, en partant de cette remarque, a fait voir que, si deux racines d'une équation irréductible sont tellement liées entre elles, que l'une puisse s'exprimer rationnellement par l'autre, on peut toujours ramener la résolution de l'équation à celle d'équations de degrés moindres. Il y a même des cas où l'équation est résoluble

algébriquement; cela arrive en particulier si son degré est un nombre premier.

Nous allons exposer ici ces recherches d'Abel, et nous ferons ensuite l'application de sa méthode aux équations dont dépend la division du cercle en un nombre premier de parties égales.

530. Soit

$$(1) \qquad f(x) = 0$$

une équation irréductible de degré μ, et supposons que deux racines x' et x_1 soient liées entre elles par l'équation

$$x' = \theta x_1,$$

où θx désigne une fonction rationnelle de x et des quantités connues. x' étant racine de l'équation (1), on aura

$$f(\theta x_1) = 0;$$

d'où il suit que x_1 est racine de l'équation

$$(2) \qquad f(\theta x) = 0,$$

et, par conséquent, cette équation (2) admet toutes les racines de l'équation (1) (n° 100), car celle-ci est irréductible, et $f(\theta x)$ est une fonction rationnelle. En d'autres termes, si x désigne une racine quelconque de l'équation (1), θx sera aussi racine de cette équation. Mais θx_1 est racine de l'équation (1); donc $\theta\theta x_1$ le sera aussi, ainsi que $\theta\theta\theta x_1$, et généralement, en répétant sur x_1 un nombre quelconque de fois l'opération désignée par θ, on obtiendra toujours une racine de l'équation (1).

Soit, pour abréger,

$$\theta\theta x_1 = \theta^2 x_1, \quad \theta\theta^2 x_1 = \theta^3 x_1, \quad \theta\theta^3 x_1 = \theta^4 x_1, \quad \ldots,$$

tous les termes de la série

$$(3) \qquad x_1, \; \theta x_1, \; \theta^2 x_1, \; \theta^3 x_1, \; \ldots$$

seront des racines de l'équation (1). Mais la série (3) renferme une infinité de termes, tandis que l'équation (1) n'a que μ racines; il faut donc que quelques-unes des quantités (3) se trouvent répétées un nombre infini de fois.

Supposons, par exemple, que l'on ait

$$\theta^{m+n} x_1 = \theta^m x_1,$$

ou

$$\theta^n (\theta^m x_1) - \theta^m x_1 = 0,$$

l'équation

$$\theta^n x - x = 0$$

a la racine $\theta^m x_1$ commune avec l'équation (1); elle admettra donc toutes les racines de l'équation (1), et l'on aura

$$\theta^n x_1 - x_1 = 0$$

ou

$$\theta^n x_1 = x_1.$$

On tire de là

$$\theta^{n+k} x_1 = \theta^k x_1;$$

d'où il suit que les termes de la série (3), à partir du $n^{\text{ième}}$, se reproduiront dans le même ordre, et que cette série ne contiendra que les n racines distinctes

$$(4) \qquad x_1, \ \theta x_1, \ \theta^2 x_1, \ \ldots, \ \theta^{n-1} x_1.$$

Ces n racines seront effectivement distinctes, si n est le nombre de fois qu'il faut répéter sur x_1 l'opération désignée par θ pour reproduire x_1.

Si l'on a $\mu = n$, la série (4) contient toutes les racines de l'équation (1).

Supposons $\mu > n$, et soit x_2 une racine de l'équation (1) qui ne fasse pas partie de la série (4), on fera voir, comme précédemment, que toutes les quantités

$$(5) \qquad x_2, \ \theta x_2, \ \theta^2 x_2, \ \ldots, \ \theta^{n-1} x_2, \ \ldots$$

sont également racines de l'équation (1). Or je dis que,

dans la série (5), les n premiers termes

(6) $$x_2,\ \theta x_2,\ \theta^2 x_2,\ \ldots,\ \theta^{n-1} x_2$$

sont les seuls qui puissent être différents. En effet, l'équation

$$\theta^n x - x = 0$$

admet la racine x_1 de l'équation (1); donc elle admettra toutes les autres, et l'on aura

$$\theta^n x_2 = x_2,$$

d'où

$$\theta^{n+k} x_2 = \theta^k x_2.$$

Par conséquent, les termes de la série (5) se reproduiront dans le même ordre, à partir du $n^{\text{ième}}$, et, parmi ces termes, les seuls qui puissent être distincts sont renfermés dans la série (6).

Je dis maintenant que les termes de la série (6) sont effectivement différents entre eux, et distincts des quantités (4).

L'égalité

$$\theta^k x_2 = \theta^i x_2,$$

où k et i sont inférieurs à n, est effectivement impossible; car, d'après le théorème établi au n° 100, elle entraînerait

$$\theta^k x_1 = \theta^i x_1,$$

ce qui n'a pas lieu, puisque les quantités (4) sont différentes.

L'égalité

$$\theta^k x_2 = \theta^i x_1$$

est de même impossible. Si, en effet, elle avait lieu, il en résulterait

$$\theta^{n-k} \theta^i x_1 = \theta^{n-k} \theta^k x_2$$

ou

$$\theta^{n-k+i} x_1 = \theta^n x_2 = x_2,$$

et, par conséquent, x_2 ferait partie de la série (4), ce qui est contre l'hypothèse.

Le nombre des racines de l'équation (1) renfermées dans les séries (4) et (6) est $2n$; on a donc nécessairement $\mu = 2n$ ou $\mu > 2n$.

Supposons $\mu > 2n$, et désignons par x_3 une racine de l'équation (1) qui ne fasse pas partie des groupes (4) et (6); en raisonnant comme précédemment, on formera un troisième groupe de n racines,

$$x_3,\ \theta x_3,\ \theta^2 x_3,\ \ldots,\ \theta^{n-1} x_3,$$

toutes distinctes et différentes des quantités (4) et (6); d'où il suit nécessairement que l'on a $\mu = 3n$ ou $\mu > 3n$.

En continuant ainsi, on verra que les μ racines de l'équation (1) peuvent être partagées en un certain nombre m de groupes composés chacun de n termes, en sorte que

$$\mu = mn.$$

Les racines de l'équation (1) seront alors

$$(7)\qquad \left\{\begin{array}{lllll} x_1, & \theta x_1, & \theta^2 x_1, & \ldots, & \theta^{n-1} x_1, \\ x_2, & \theta x_2, & \theta^2 x_2, & \ldots, & \theta^{n-1} x_2, \\ x_3, & \theta x_3, & \theta^2 x_3, & \ldots, & \theta^{n-1} x_3, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ x_m, & \theta x_m, & \theta^2 x_m, & \ldots, & \theta^{n-1} x_m. \end{array}\right.$$

531. Considérons l'équation de degré n qui a pour racines les racines de l'un de ces groupes, du premier par exemple, et soit

$$(x - x_1)(x - \theta x_1)(x - \theta^2 x_1)\ldots(x - \theta^{n-1} x_1) = 0$$

ou

$$(8)\qquad x^n + A_1^{(1)} x^{n-1} + A_2^{(1)} x^{n-2} + \ldots + A_{n-1}^{(1)} x + A_n^{(1)} = 0$$

cette équation. Les coefficients

$$A_1^{(1)},\ A_2^{(1)},\ \ldots,\ A_m^{(1)}$$

sont des fonctions rationnelles et symétriques des quantités

$$x_1,\ \theta x_1,\ \theta^2 x_1,\ \ldots,\ \theta^{n-1} x_1,$$

et ils ne dépendent, comme on va voir, que d'une seule équation du degré m.

Soit, en effet, y_1 une fonction rationnelle et symétrique quelconque des quantités

$$(9)\qquad x_1,\ \theta x_1,\ \theta^2 x_1,\ \ldots,\ \theta^{n-1} x_1;$$

θx_1, $\theta^2 x_1$, ... étant des fonctions rationnelles de x_1, y_1 le sera aussi, et nous poserons

$$y_1 = F(x_1),$$

F désignant une fonction rationnelle. En outre, à cause de $\theta^n x_1 = x_1$, les quantités (9) ne feront que se changer les unes dans les autres si l'on remplace x_1 par θx_1, $\theta^2 x_1$, ..., $\theta^{n-1} x_1$; et comme y_1 est une fonction symétrique de ces quantités, sa valeur sera invariable par ces changements; on aura donc

$$y_1 = F(x_1) = F(\theta x_1) = F(\theta^2 x_1) = \ldots = F(\theta^{n-1} x_1).$$

Désignons par

$$y_2,\ y_3,\ \ldots,\ y_m$$

les valeurs que prend y_1 quand on y remplace x_1 successivement par

$$x_2,\ x_3,\ \ldots,\ x_m;$$

on aura

$$y_1 = F(x_2) = F(\theta x_2) = F(\theta^2 x_2) = \ldots = F(\theta^{n-1} x_2),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$y_m = F(x_m) = F(\theta x_m) = F(\theta^2 x_m) = \ldots = F(\theta^{n-1} x_m).$$

Soit maintenant

$$(y-y_1)(y-y_2)\ldots(y-y_m)=0$$

ou

$$(10)\quad y^m+p_1y^{m-1}+p_2y^{m-2}+\ldots+p_{m-1}y+p_m=0$$

l'équation qui a pour racines $y_1, y_2, \ldots, y_m$; je dis que les coefficients p_1, p_2, ... de cette équation peuvent être exprimés rationnellement par les coefficients de l'équation proposée (1). On a, en effet, quel que soit l'entier λ,

$$y_1^\lambda=\frac{1}{n}\left\{[F(x_1)]^\lambda+[F(\theta x_1)]^\lambda+\ldots+[F(\theta^{n-1}x_1)]^\lambda\right\},$$

$$y_2^\lambda=\frac{1}{n}\left\{[F(x_2)]^\lambda+[F(\theta x_2)]^\lambda+\ldots+[F(\theta^{n-1}x_2)]^\lambda\right\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$y_m^\lambda=\frac{1}{n}\left\{[F(x_m)]^\lambda+[F(\theta x_m)]^\lambda+\ldots+[F(\theta^{n-1}x_m)]^\lambda\right\},$$

et, en ajoutant,

$$y_1^\lambda+y_2^\lambda+\ldots+y_m^\lambda=\frac{1}{n}\sum[F(x)]^\lambda.$$

Le signe $\sum$ du second membre s'étend à toutes les racines de l'équation proposée; ce second membre est donc une fonction symétrique et rationnelle de toutes les racines; d'où il résulte que les sommes de puissances semblables des racines de l'équation (10) peuvent être exprimées rationnellement par les coefficients de l'équation proposée. On pourra donc aussi exprimer de la même manière les coefficients p_1, p_2, ..., ainsi que nous l'avions annoncé.

La fonction rationnelle et symétrique y_1 des quantités (9), fonction qui peut être choisie à volonté, dépend donc directement d'une équation de degré m. D'ailleurs

les fonctions

$$y_1,\ A_1^{(1)},\ A_2^{(1)},\ \ldots,\ A_n^{(1)}$$

sont semblables; car elles peuvent toutes être considérées comme des fonctions rationnelles de la seule racine x_1. On pourra donc exprimer

$$A_1^{(1)},\ A_2^{(1)},\ \ldots,\ A_n^{(1)}$$

en fonction rationnelle de y_1.

Nous sommes ainsi conduits à l'une des applications les plus importantes de la théorie des fonctions semblables, que nous avons développée dans le Chapitre V de la Section IV; mais, comme cette théorie est sujette à quelques cas d'exception, il ne sera pas inutile d'entrer, avec Abel, dans le détail du calcul des coefficients $A_1^{(1)}$, $A_2^{(1)}$, ...

Désignons par $\psi(x_1)$ l'un quelconque de ces coefficients; ψ est une fonction rationnelle qui ne doit pas changer quand on remplace x_1 par $\theta x_1, \theta^2 x_1, \ldots, \theta^{n-1} x_1$, puisque $\psi(x_1)$ est, comme y_1, une fonction symétrique des quantités (9); et il en sera de même de la fonction

$$y_1^\lambda \psi(x_1) \quad \text{ou} \quad [F(x_1)]^\lambda \psi(x_1).$$

On aura donc

$$y_1^\lambda \psi(x_1) = \frac{1}{n}\Big\{[F(x_1)]^\lambda \psi(x_1) + [F(\theta x_1)]^\lambda \psi(\theta x_1) + \ldots \\ + [F(\theta^{n-1} x_1)]^\lambda \psi(\theta^{n-1} x_1)\Big\},$$

en remplaçant x_1 successivement par $x_2, x_3, \ldots, x_m$, on aura des expressions semblables pour $y_2^\lambda \psi(x_2), \ldots, y_m^\lambda \psi(x_m)$; et, si l'on pose

$$(11) \qquad t_\lambda = y_1^\lambda \psi(x_1) + y_2^\lambda \psi(x_2) + \ldots + y_m^\lambda \psi(x_m),$$

on aura

$$t_\lambda = \frac{1}{n}\sum [F(x)]^\lambda \psi(x),$$

le signe $\sum$ s'étendant à toutes les racines de l'équation (1). On voit par là que t_λ est une fonction symétrique et rationnelle des racines de l'équation (1), qui pourra, par conséquent, s'exprimer rationnellement en fonction des quantités connues.

Cela posé, en prenant pour λ les valeurs 0, 1, 2, 3, ..., $(m-1)$, l'équation (11) donnera les suivantes :

$$(12)\quad \begin{cases} \psi(x_1) + \psi(x_2) + \ldots + \psi(x_m) = t_0, \\ y_1\psi(x_1) + y_2\psi(x_2) + \ldots + y_m\psi(x_m) = t_1, \\ y_1^2\psi(x_1) + y_2^2\psi(x_2) + \ldots + y_m^2\psi(x_m) = t_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ y_1^{m-1}\psi(x_1) + y_2^{m-1}\psi(x_2) + \ldots + y_m^{m-1}\psi(x_m) = t_{m-1}, \end{cases}$$

dont les seconds membres peuvent être considérés comme connus.

Pour avoir la valeur de $\psi(x_1)$, ajoutons les équations (12), après les avoir respectivement multipliées par les indéterminées

$$R_0,\ R_1,\ \ldots,\ R_{m-2},\ 1,$$

et faisons, pour abréger,

$$(13)\quad \varphi(y) = y^{m-1} + R_{m-2}y^{m-2} + \ldots + R_1 y + R_0,$$

on aura

$$\varphi(y_1)\psi(x_1) + \varphi(y_2)\psi(x_2) + \ldots + \varphi(y_m)\psi(x_m)$$
$$= t_0 R_0 + t_1 R_1 + \ldots + t_{m-2} R_{m-2} + t_{m-1};$$

et, si l'on détermine les facteurs R_0, R_1, ... par les conditions

$$\varphi(y_2) = 0,\quad \varphi(y_3) = 0,\quad \ldots,\quad \varphi(y_m) = 0,$$

on aura

$$(14)\quad \psi(x_1) = \frac{t_0 R_0 + t_1 R_1 + \ldots + t_{m-2} R_{m-2} + t_{m-1}}{\varphi(y_1)}.$$

Cherchons maintenant les valeurs de R_0, R_1, ... D'après notre hypothèse, l'équation

$$\varphi(y) = 0$$

doit avoir pour racines $y_2, y_3, \ldots, y_m$; mais ces racines appartiennent aussi à l'équation (10), qui admet en outre la racine y_1 : on aura donc

$$(15)\quad \left\{ \begin{array}{l} \varphi(y) = \dfrac{y^m + p_1 y^{m-1} + p_2 y^{m-2} + \ldots + p_{m-1} y + p_m}{y - y_1} \\ \quad = y^{m-1} + \begin{array}{l|l|l} p_1 & y^{m-2} + p_2 & y^{m-3} + \ldots + p_{m-1} \\ + y_1 & \quad + p_1 y_1 & \quad + p_{m-2} y_1 \\ & \quad + y_1^2 & \quad + \ldots\ldots \\ & & \quad \ldots\ldots\ldots \\ & & \quad + p_1 y_1^{m-2} \\ & & \quad + y^{m-1}. \end{array} \end{array} \right.$$

Comparant les valeurs $\varphi(y)$ données par les équations (13) et (15), on trouve

$$(16)\quad \left\{ \begin{array}{l} R_{m-2} = p_1 + y_1, \\ R_{m-3} = p_2 + p_1 y_1 + y_1^2, \\ \ldots\ldots\ldots\ldots\ldots\ldots, \\ R_1 = p_{m-2} + p_{m-3} y_1 + \ldots + y^{m-2}, \\ R_0 = p_{m-1} + p_{m-2} y_1 + \ldots + y_1^{m-1}. \end{array} \right.$$

On tire aussi de l'équation (15)

$$\varphi(y_1) = m y_1^{m-1} + (m-1) p_1 y_1^{m-2} + \ldots + 2 p_{m-2} y_1 + p_{m-1},$$

et en faisant, pour abréger,

$$\begin{array}{l} T_0 = t_0 p_{m-1} + t_1 p_{m-2} + \ldots + t_{m-2} p_1 + t_{m-1}, \\ T_1 = t_0 p_{m-2} + t_1 p_{m-3} + \ldots + t_{m-2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ T_{m-2} = t_0 p_1 + t_1, \\ T_{m-1} = t_0, \end{array}$$

on aura cette valeur de $\psi(x_1)$,

$$(17)\quad \psi(x_1)=\frac{T_{m-1}y_1^{m-1}+T_{m-2}y_1^{m-2}+\ldots+T_1y_1+T_0}{my_1^{m-1}+(m-1)p_1y_1^{m-2}+\ldots+2p_{m-2}y_1+p_{m-1}}.$$

La formule précédente n'est en défaut que si le dénominateur du second membre est nul. Or, je dis qu'on peut toujours faire en sorte que cela ne soit pas. En effet, ce dénominateur est égal au produit

$$(y_1-y_2)(y_1-y_3)\ldots(y_1-y_m),$$

et, pour qu'il soit nul, il faut que l'un des facteurs le soit, que l'on ait, par exemple,

$$y_1=y_k.$$

Cela posé, prenons pour y_1 la fonction

$$y_1=(\alpha-x_1)(\alpha-\theta x_1)(\alpha-\theta^2x_1)\ldots(\alpha-\theta^{n-1}x_1),$$

α étant indéterminé; l'équation $y_1=y_k$, ou

$$(\alpha-x_1)(\alpha-\theta x_1)\ldots=(\alpha-x_k)(\alpha-\theta x_k)\ldots,$$

ne peut avoir lieu, quel que soit α, à moins d'être identique; ce qui est impossible, puisque les quantités x_k, θx_k, ... sont différentes de x_1, θx_1, ... D'où il suit qu'en choisissant y_1, comme il vient d'être dit, l'équation (17) donnera pour $\psi(x_1)$ une valeur finie et déterminée.

Les coefficients $A_1^{(1)}$, $A_2^{(1)}$, ... de l'équation (8) peuvent donc s'exprimer rationnellement par une même fonction y_1 dont la valeur dépend d'une équation du degré m; et si l'on remplace y_1 successivement par $y_2, y_3, \ldots, y_m$, on aura m équations du degré n, dont les racines seront respectivement

$$\begin{array}{llll} x_1, & \theta x_1, & \ldots, & \theta^{n-1}x_1,\\ x_2, & \theta x_2, & \ldots, & \theta^{n-1}x_2,\\ \ldots & \ldots & \ldots & \ldots,\\ x_m, & \theta x_m, & \ldots, & \theta^{n-1}x_m, \end{array}$$

d'où il suit que l'équation proposée peut être décomposée en m équations chacune du degré n, dont les coefficients sont respectivement des fonctions rationnelles d'une même racine d'une équation du degré m.

Cette dernière équation n'est pas en général résoluble algébriquement, quand son degré surpasse le quatrième; mais l'équation (8) et les autres semblables le sont toujours, comme nous allons le démontrer, en supposant connus les coefficients $A_1^{(1)}, A_1^{(2)}, \ldots$. Dans cette hypothèse, notre analyse ramène la résolution de l'équation proposée de degré $\mu = mn$ à celle de m équations de degré n, qui ont cette propriété, que toutes les racines de chacune d'elles peuvent être représentées par

$$x,\ \theta x,\ \theta^2 x,\ \ldots,\ \theta^{n-1} x.$$

Résolution algébrique des équations dont toutes les racines peuvent être représentées par x, θx, $\theta^2 x$, ..., $\theta^{\mu-1} x$, θx étant une fonction rationnelle de x et des quantités connues, telle que $\theta^\mu x = x$.

532. Soit

$$(1) \qquad f(x) = 0$$

une équation de degré μ, dont les racines sont

$$x,\ \theta x,\ \theta^2 x,\ \ldots,\ \theta^{\mu-1} x,$$

θx désignant une fonction rationnelle de x et des quantités connues, telle que l'on ait

$$(2) \qquad \theta^\mu x = x,$$

et, par conséquent,

$$(3) \qquad \theta^{\mu+k} x = \theta^k x.$$

Désignons par α une racine quelconque de l'équation

$$x^\mu = 1,$$

et posons, avec Lagrange (n° 520),

$$(4)\qquad \psi(x) = (x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1}x)^\mu;$$

je dis que la fonction $\psi(x)$ est exprimable rationnellement par les quantités connues de $f(x)$ et de $\theta(x)$.

En effet, remplaçons x par $\theta^m x$ dans l'équation (4), on aura

$$\psi(\theta^m x) = (\theta^m x + \alpha\theta^{m+1}x + \alpha^2\theta^{m+2}x + \ldots + \alpha^{\mu-1}\theta^{m+\mu-1}x)^\mu,$$

et, en ayant égard aux équations (2) et (3),

$$\begin{aligned}\psi(\theta^m x) &= (\theta^m x + \alpha\theta^{m+1}x + \ldots + \alpha^{\mu-m}x + \alpha^{\mu-m+1}\theta x + \ldots + \alpha^{\mu-1}\theta^{m-1}x)^\mu\\ &= (\alpha^{\mu-m}x + \alpha^{\mu-m+1}\theta x + \ldots + \alpha^{\mu-1}\theta^{m-1}x + \theta^m x + \ldots + \alpha^{\mu-m-1}\ldots\\ &= (\alpha^{\mu-m})^\mu(x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1}x)^\mu,\end{aligned}$$

ou enfin, à cause de $\alpha^\mu = 1$,

$$\psi(\theta^m x) = \psi(x).$$

Donnant à m les valeurs successives $0, 1, 2, \ldots, \mu-1$, on a

$$\psi(x) = \psi(\theta x) = \psi(\theta^2 x) = \ldots = \psi(\theta^{\mu-1}x),$$

et, par conséquent,

$$\psi(x) = \frac{1}{\mu}[\psi(x) + \psi(\theta x) + \ldots + \psi(\theta^{\mu-1}x)];$$

d'où il suit que $\psi(x)$ est une fonction rationnelle et symétrique de toutes les racines de l'équation (1); elle pourra donc être exprimée rationnellement par les coefficients de cette équation.

Posons alors

$$\psi(x) = v,$$

on aura

$$x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1}x = \sqrt[\mu]{v},$$

v étant une quantité connue. Et si l'on désigne par

$$1,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{\mu-1}$$

les μ racines de l'équation

$$x^\mu = 1,$$

par

$$v_0,\ v_1,\ v_2,\ \ldots,\ v_{\mu-1}$$

les valeurs correspondantes de v, on aura

$$(5)\quad \begin{cases} x + \theta x + \theta^2 x + \ldots\ldots\ldots\ldots\ldots + \theta^{\mu-1}x = \sqrt[\mu]{v_0}, \\ x + \alpha_1\theta x + \alpha_1^2\theta^2 x + \ldots\ldots\ldots + \alpha_1^{\mu-1}\theta^{\mu-1}x = \sqrt[\mu]{v_1}, \\ x + \alpha_2\theta x + \alpha_2^2\theta^2 x + \ldots\ldots\ldots + \alpha_2^{\mu-1}\theta^{\mu-1}x = \sqrt[\mu]{v_2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x + \alpha_{\mu-1}\theta x + \alpha_{\mu-1}^2\theta^2 x + \ldots + \alpha_{\mu-1}^{\mu-1}\theta^{\mu-1}x = \sqrt[\mu]{v_{\mu-1}}. \end{cases}$$

La quantité $\sqrt[\mu]{v_0}$ est immédiatement donnée par l'équation (1); car, si l'on désigne par A le coefficient de $x^{\mu-1}$ dans cette équation, on a

$$\sqrt[\mu]{v_0} = -\mathrm{A}.$$

En ajoutant les équations (5), et ayant égard aux propriétés connues des racines α, il vient

$$(6)\qquad x = \frac{-\mathrm{A} + \sqrt[\mu]{v_1} + \sqrt[\mu]{v_2} + \ldots + \sqrt[\mu]{v_{\mu-1}}}{\mu};$$

et l'on aura généralement la valeur d'une racine quel-

conque $\theta^m x$, en ajoutant les équations (5) respectivement multipliées par

$$1,\ \alpha_1^{-m},\ \alpha_2^{-m},\ \alpha_3^{-m},\ \ldots,\ \alpha_{\mu-1}^{-m};$$

on trouve ainsi

$$(7)\quad \theta^m x = \frac{-A + \alpha_1^{-m}\sqrt[\mu]{v_1} + \alpha_2^{-m}\sqrt[\mu]{v_2} + \ldots + \alpha_{\mu-1}^{-m}\sqrt[\mu]{v_{\mu-1}}}{\mu},$$

cette formule donnera les valeurs de θx, $\theta^2 x$, ..., $\theta^{\mu-1}x$, en attribuant à m les valeurs 1, 2, 3, ..., $(\mu - 1)$.

533. Dans l'équation (6) et dans toutes celles qu'on déduit de la formule (7), on doit considérer chaque radical $\sqrt[\mu]{v_1}$, $\sqrt[\mu]{v_2}$, ..., $\sqrt[\mu]{v_{\mu-1}}$ comme ayant toujours la même valeur. Si on laisse à ces radicaux toute leur généralité, l'équation (7) ne diffère aucunement de l'équation (6), et cette dernière renferme l'expression de toutes les racines. Il y a en outre ici une difficulté, car l'équation (6) donne pour x une expression qui a $\mu^{\mu-1}$ valeurs, tandis que l'équation (1) n'a que μ racines. Mais nous avons déjà eu l'occasion d'indiquer comment on peut faire disparaître cette ambiguïté, et il est facile d'établir que, quand on a fixé la valeur de l'un des radicaux, les autres sont par cela même déterminés.

En effet, désignons par α une racine primitive de l'équation

$$\alpha^\mu = 1,$$

et posons

$$\alpha_1 = \alpha,\quad \alpha_2 = \alpha^2,\quad \alpha_3 = \alpha^3,\quad \ldots,\quad \alpha_{\mu-1} = \alpha^{\mu-1};$$

on aura

$$\sqrt[\mu]{v_1} = x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta^{\mu-1}x,$$

$$\sqrt[\mu]{v_n} = x + \alpha^n\theta x + \alpha^{2n}\theta^2 x + \ldots + \alpha^{(\mu-1)n}\theta^{\mu-1}x.$$

Si l'on change x en $\theta^m x$, $\sqrt[\mu]{v_1}$ se changera en $\alpha^{\mu-m}\sqrt[\mu]{v_1}$, ainsi qu'on le reconnaît par le calcul effectué plus haut. Pareillement $\sqrt[\mu]{v_n}$ sera, par le même changement de x en $\theta^m x$, multiplié par $\alpha^{n(\mu-m)}$; d'où il suit que le produit

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n}$$

sera multiplié par $\alpha^{\mu(\mu-m)} = 1$, c'est-à-dire qu'il n'éprouvera aucun changement. Si donc on pose

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n} = \varphi(x),$$

on aura

$$\varphi(x) = \varphi(\theta x) = \varphi(\theta^2 x) = \ldots = \varphi(\theta^{\mu-1} x),$$

et, par conséquent,

$$\varphi(x) = \frac{1}{\mu}\left[\varphi(x) + \varphi(\theta x) + \ldots + \varphi(\theta^{\mu-1} x)\right].$$

$\varphi(x)$ est donc une fonction rationnelle et symétrique des racines de l'équation (1), et l'on pourra l'exprimer rationnellement par les quantités connues; en désignant par a_n sa valeur, on aura

$$\sqrt[\mu]{v_n}\left(\sqrt[\mu]{v_1}\right)^{\mu-n} = a_n,$$

ou

$$\sqrt[\mu]{v_n} = \frac{a_n}{v_1}\left(\sqrt[\mu]{v_1}\right)^n.$$

On pourra exprimer ainsi chacun des radicaux $\sqrt[\mu]{v_2}$, $\sqrt[\mu]{v_3}$, ... en fonction rationnelle de $\sqrt[\mu]{v_1}$, et l'équation (6) prendra la forme

$$) \quad x = \frac{1}{\mu}\left[-A + \sqrt[\mu]{v_1} + \frac{a_2}{v_1}\left(\sqrt[\mu]{v_1}\right)^2 + \frac{a_3}{v_1}\left(\sqrt[\mu]{v_1}\right)^3 + \ldots + \frac{a_{\mu-1}}{v_1}\left(\sqrt[\mu]{v_1}\right)^{\mu-1}\right].$$

Cette expression de x a précisément μ valeurs, et elle représente bien les μ racines de l'équation proposée.

De ce qui précède on peut conclure cette proposition :

Théorème I. — *Si les μ racines d'une équation quelconque peuvent être représentées par*

$$x,\ \theta x,\ \theta^2 x,\ \ldots,\ \theta^{\mu-1} x,$$

θx étant une fonction rationnelle telle que $\theta^\mu = x$, l'équation est toujours soluble par radicaux.

Et en rapprochant cet énoncé du théorème démontré au n° 531, on a cet autre théorème :

Théorème II. — *Si deux racines d'une équation irréductible de degré premier sont telles, que l'une puisse s'exprimer rationnellement en fonction de l'autre, l'équation est soluble par radicaux.*

Cas où les quantités connues sont réelles.

534. Si tous les coefficients de f et de θ sont réels, on a un théorème remarquable, que Gauss a établi le premier à l'égard des équations dont dépend la division du cercle en parties égales.

Nous avons posé précédemment

$$v_1 = (x + \alpha\theta x + \alpha^2\theta^2 x + \ldots + \alpha^{\mu-1}\theta_{\mu-1} x)^\mu,$$

et nous avons établi que v_1 est une fonction symétrique des racines de l'équation $f(x) = 0$; par conséquent v_1 est exprimable rationnellement par les coefficients de f et de θ; et si ces quantités sont toutes réelles, v_1 ne contiendra d'autres imaginaires que celle de la racine α. En outre, $v_{\mu-1}$ se déduit de v_1 en remplaçant α par l'expression conjuguée $\alpha^{\mu-1}$; d'où il résulte que v_1 et $v_{\mu-1}$

sont des quantités connues imaginaires et conjuguées. On pourra donc poser

$$(1)\qquad \begin{cases} v_1 = \rho(\cos\omega + \sqrt{-1}\sin\omega), \\ v_{\mu-1} = \rho(\cos\omega - \sqrt{-1}\sin\omega). \end{cases}$$

Nous avons aussi, en général,

$$\left(\sqrt[\mu]{v_1}\right)^{\mu-n}\sqrt[\mu]{v_n} = a_n,$$

et, pour $n = \mu - 1$,

$$(2)\qquad \sqrt[\mu]{v_1}\sqrt[\mu]{v_{\mu-1}} = a_{\mu-1}.$$

$a_{\mu-1}$ est exprimable rationnellement par les coefficients de f et de θ : elle ne peut donc renfermer d'autres imaginaires que celle qui se trouve dans α. Mais il est évident que $a_{\mu-1}$ ne change pas si l'on remplace α par $\alpha^{\mu-1}$ qui est sa conjuguée ; donc $a_{\mu-1}$ est réelle.

Des équations (1) et (2) on déduit

$$\rho^2 = a_{\mu-1}^\mu,$$

et, en désignant par a la valeur numérique de $a_{\mu-1}$,

$$\sqrt[\mu]{\rho} = \sqrt{a}.$$

La première des équations (1) donne alors cette valeur de $\sqrt[\mu]{v_1}$,

$$\sqrt[\mu]{v_1} = \sqrt{a}\left(\cos\frac{\omega + 2k\pi}{\mu} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{\mu}\right),$$

où k désigne un nombre entier, et l'expression des racines x, donnée par l'équation (8) du n° 533, prend

cette forme très-remarquable :

$$x = \frac{1}{\mu}\left\{ -A + \sqrt{a}\left(\cos\frac{\omega + 2k\pi}{\mu} + \sqrt{-1}\sin\frac{\omega + 2k\pi}{\mu}\right)\right.$$
$$+ (f + g\sqrt{-1}) \quad \left[\cos\frac{2(\omega + 2k\pi)}{\mu} + \sqrt{-1}\sin\frac{2(\omega + 2k\pi)}{\mu}\right]$$
$$+ (f_1 + g_1\sqrt{-1})\sqrt{a}\left[\cos\frac{3(\omega + 2k\pi)}{\mu} + \sqrt{-1}\sin\frac{3(\omega + 2k\pi)}{\mu}\right]$$
$$+ (f_2 + g_2\sqrt{-1}) \quad \left[\cos\frac{4(\omega + 2k\pi)}{\mu} + \sqrt{-1}\sin\frac{4(\omega + 2k\pi)}{\mu}\right]$$
$$\left. + \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \right\},$$

où $a, f, g, f_1, g_1, \ldots$ sont des fonctions rationnelles de $\cos\frac{2\pi}{\mu}$ et de $\sin\frac{2\pi}{\mu}$.

La formule précédente fera connaître les μ racines de $f(x) = 0$, si l'on donne au nombre entier k les μ valeurs $0, 1, 2, 3, \ldots, \mu - 1$. De là résulte le théorème suivant :

Théorème. — *Pour résoudre l'équation proposée $f(x) = 0$, il suffit :*

1° De diviser la circonférence entière du cercle en μ parties égales; 2° de diviser ensuite un angle ω qu'on peut construire en μ parties égales; 3° d'extraire la racine carrée d'une seule quantité a.

Remarque. — Les coefficients de f et de θ étant tous réels, si une racine de $f(x) = 0$ est réelle, toutes les autres le sont aussi, puisque, si x désigne cette racine réelle, les autres racines sont

$$\theta x,\ \theta^2 x,\ \ldots,\ \theta^{\mu-1} x;$$

par conséquent, les racines de l'équation proposée sont toutes réelles, ou toutes imaginaires.

Première méthode particulière relative aux équations abéliennes dont le degré est un nombre composé.

535. La méthode qui vient d'être exposée pour la résolution algébrique de l'équation abélienne de degré μ,

$$(1) \qquad f(x) = 0,$$

est applicable à tous les cas, que μ soit premier ou non; mais, quand μ est un nombre composé, on peut simplifier la solution en opérant comme nous allons l'indiquer.

Soit $\mu = mn$. Les racines de l'équation (1) étant toujours

$$x, \quad \theta x, \quad \theta^2 x, \quad \ldots, \quad \theta^{\mu-1} x,$$

nous pourrons les partager en m groupes de la manière suivante :

$$\begin{array}{lllll} x, & \theta^m x, & \theta^{2m} x, & \ldots, & \theta^{(n-1)m} x, \\ \theta x, & \theta^{m+1} x, & \theta^{2m+1} x, & \ldots, & \theta^{(n-1)m+1} x, \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots, \\ \theta^{m-1} x, & \theta^{2m-1} x, & \theta^{3m-1} x, & \ldots, & \theta^{nm-1} x; \end{array}$$

ou, en posant

$$x = x_1, \quad \theta x = x_2, \quad \theta^2 x = x_3, \quad \ldots, \quad \theta^{m-1} x = x_m$$

et

$$\theta^m x = \theta_1 x,$$

de la manière suivante :

$$(2) \qquad \left\{ \begin{array}{lllll} x_1, & \theta_1 x_1, & \theta_1^2 x_1, & \ldots, & \theta_1^{n-1} x_1, \\ x_2, & \theta_1 x_2, & \theta_1^2 x_2, & \ldots, & \theta_1^{n-1} x_2, \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots & \ldots\ldots, \\ x_m, & \theta_1 x_m, & \theta_1^2 x_m, & \ldots, & \theta_1^{n-1} x_m. \end{array} \right.$$

En appliquant donc à l'équation (1) la méthode exposée au n° 531, on pourra la décomposer en m équations,

chacune du degré n, qui auront respectivement pour racines les racines des divers groupes (2), et dont les coefficients seront des fonctions rationnelles d'une même racine d'une équation

$$(3) \qquad \psi(y) = 0$$

de degré m. Soient

$$y_1, y_2, \ldots, y_m$$

les m racines de l'équation (3), et

$$(4) \qquad \varphi(x, y_1) = 0, \quad \varphi(x, y_2) = 0, \quad \ldots, \quad \varphi(x, y_m) = 0$$

les m équations qui ont respectivement pour racines les quantités du premier groupe (2), du deuxième, etc., du dernier. Je dis que, pour résoudre l'équation (1), il suffit de connaître une racine y de l'équation (3), et ensuite une racine x de l'équation

$$(5) \qquad \varphi(x, y) = 0$$

correspondante; car on aura, de cette manière, une première racine x de l'équation (1), et les autres seront

$$\theta x, \ \theta^2 x, \ \ldots, \ \theta^{\mu-1} x.$$

L'équation proposée (1) étant résoluble algébriquement, l'équation (3) l'est aussi; car y désigne une fonction rationnelle de x. Mais je dis en outre que l'équation (3) jouit de la même propriété que l'équation (1), et que, par conséquent, on pourra lui appliquer la même méthode de résolution.

En effet, les racines de l'équation (1), renfermées dans le premier des groupes (2), sont

$$(6) \qquad x, \ \theta^m x, \ \theta^{2m} x, \ \ldots, \ \theta^{(n-1)m} x,$$

et y désigne une fonction rationnelle et symétrique de ces racines, c'est-à-dire une fonction rationnelle de x.

Posons

$$y = \mathfrak{F}[x, \theta^m x, \theta^{2m} x, \ldots, \theta^{(n-1)m} x] = \mathrm{F}(x),$$

les m racines $y_1, y_2, \ldots, y_m$ de l'équation (3) seront

$$\mathrm{F}(x), \ \mathrm{F}(\theta x), \ \mathrm{F}(\theta^2 x), \ \ldots, \ \mathrm{F}(\theta^{m-1} x),$$

et l'on aura

$$\mathrm{F}(\theta x) = \mathfrak{F}(\theta x, \theta\theta^m x, \theta\theta^{2m} x, \ldots, \theta\theta^{(n-1)m} x).$$

Par conséquent, $\mathrm{F}(\theta x)$ et $\mathrm{F}(x)$ sont des fonctions rationnelles et symétriques des quantités (6), et l'on pourra exprimer rationnellement l'une par l'autre en appliquant la méthode des fonctions semblables rappelée au n° 531.

Soit donc

$$\mathrm{F}(\theta x) = \lambda \mathrm{F}(x) = \lambda y;$$

λy étant une fonction rationnelle de y, on aura

$$\mathrm{F}(\theta^2 x) = \lambda \mathrm{F}(\theta x) = \lambda^2 y,$$
$$\mathrm{F}(\theta^3 x) = \lambda \mathrm{F}(\theta^2 x) = \lambda^3 y,$$
$$\cdots\cdots\cdots\cdots\cdots,$$
$$\mathrm{F}(\theta^{m-1} x) = \lambda \mathrm{F}(\theta^{m-2} x) = \lambda^{m-1} y,$$

et l'on voit que les m racines de l'équation (3) pourront être représentées par

$$y, \ \lambda y, \ \lambda^2 y, \ \ldots, \ \lambda^{m-1} y,$$

λ désignant une fonction rationnelle telle que

$$\lambda^m y = y.$$

Quand l'équation (3) sera résolue, y sera connue, et l'on pourra appliquer à l'équation (5) la méthode précédemment exposée, puisque ses n racines peuvent être représentées par

$$x, \ \theta_1 x, \ \theta_1^2 x, \ \ldots, \ \theta_1^{n-1} x.$$

On peut donc énoncer cette proposition :

Si $\mu = mn$, la résolution de l'équation (1) *est ra-*

menée à celle de deux équations des degrés m et n respectivement, et qui ont la même propriété que la proposée.

Si n est lui-même un nombre composé $m_1 n_1$, on ramènera, de la même manière, la résolution de l'équation (5) à celle d'une équation en z

$$(7) \qquad \psi_1(z, y) = 0$$

de degré m_1, et à celle d'une équation en x de degré n_1

$$(8) \qquad \varphi_1(x, y, z) = 0.$$

Dans l'équation (7), y fait partie des quantités connues, et dans l'équation (8) il en est de même de y et de z, et, généralement, on a ce théorème :

Théorème. — *Si $\mu = m_1 m_2 \ldots m_n$, la résolution de l'équation* (1) *peut être ramenée à celle de n équations des degrés*

$$m_1, \; m_2, \; \ldots, \; m_n,$$

respectivement, et il suffit même de connaître une racine de chacune de ces équations, lesquelles ont toutes la même propriété que l'équation proposée.

Corollaire I. — *Si, en décomposant μ en facteurs premiers, on a*

$$\mu = \varepsilon_1^{p_1} \varepsilon_2^{p_2} \ldots \varepsilon_\omega^{p_\omega},$$

la résolution de l'équation proposée de degré μ se ramènera à celle de p_1 équations du degré ε_1, de p_2 équations du degré ε_2, ..., de p_ω équations du degré ε_ω.

Corollaire II. — *Toute équation de degré 2^p, dont les racines peuvent être représentées par*

$$x, \; \theta x, \; \theta^2 x, \; \ldots, \; \theta^{2^p - 1} x,$$

peut être résolue à l'aide de p extractions de racines carrées.

536. Exemple. — Supposons $\mu = 30$, les racines de l'équation

$$(1) \qquad f(x) = 0$$

seront

$$x,\ \theta x,\ \theta^2 x,\ \ldots,\ \theta^{29} x.$$

Comme $30 = 2 \times 15$, on prendra pour y une fonction rationnelle et symétrique des quinze racines

$$x,\ \theta^2 x,\ \theta^4 x,\ \ldots,\ \theta^{28} x;$$

y dépendra d'une équation du deuxième degré

$$(2) \qquad y^2 + Ay + B = 0,$$

dont les coefficients seront exprimables rationnellement par ceux de la proposée; on pourrait former ensuite l'équation du quinzième degré ayant pour racines x, $\theta^2 x$, ..., $\theta^{28} x$, mais il est inutile de faire ce calcul : représentons, comme précédemment, par

$$\varphi(x, y) = 0$$

cette équation, où y est une quantité connue. Comme $15 = 3 \times 5$, on prendra pour z une fonction rationnelle et symétrique des cinq racines

$$x,\ \theta^6 x,\ \theta^{12} x,\ \theta^{18} x,\ \theta^{24} x;$$

z dépendra d'une équation du troisième degré

$$(3) \qquad z^3 + Cz^2 + Dz + E = 0,$$

dont les coefficients seront des fonctions rationnelles de y et des autres quantités connues; enfin on formera l'équation

$$(4) \qquad x^5 + Fx^4 + Gx^3 + Hx^2 + Kx + L = 0,$$

qui a pour racines

$$x,\ \theta^6 x,\ \theta^{12} x,\ \theta^{18} x,\ \theta^{24} x,$$

et dont les coefficients seront des fonctions rationnelles de y et de z. Ainsi, pour résoudre l'équation (1), il suffira de déterminer une racine de l'équation (2), puis une racine de l'équation (3), puis enfin une racine de l'équation (4).

Deuxième méthode.

537. Revenons au cas général, et supposons

$$\mu = m_1 m_2 \ldots m_\omega.$$

Désignons par n_1, n_2, ..., n_ω les quotients respectifs de μ par m_1, m_2, ..., m_ω, on aura

$$\mu = m_1 n_1 = m_2 n_2 = m_3 n_3 = \ldots = m_\omega n_\omega.$$

Cela posé, on peut, d'après ce qui précède, ramener la résolution de l'équation

$$f(x) = 0$$

à celle de deux équations, des ω manières suivantes :

(1) $\varphi_1(x, y_1) = 0$ ayant pour racines x, $\theta^{m_1}x$, $\theta^{2m_1}x$, ..., $\theta^{(n_1-1)m_1}x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_1 d'une équation $\psi_1(y_1) = 0$ de degré m_1;

(2) $\varphi_2(x, y_2) = 0$ ayant pour racines x, $\theta^{m_2}x$, $\theta^{2m_2}x$, ..., $\theta^{(n_2-1)m_2}x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_2 d'une équation $\psi_2(y_2) = 0$ de degré m_2;

....,

(ω) $\varphi_\omega(x, y_\omega) = 0$ ayant pour racines x, $\theta^{m_\omega}x$, $\theta^{2m_\omega}x$, ..., $\theta^{(n_\omega-1)m_\omega}x$, et dont les coefficients sont des fonctions rationnelles d'une racine y_ω d'une équation $\psi_\omega(y_\omega) = 0$ de degré m_ω.

Supposons maintenant que $m_1, m_2, \ldots, m_\omega$ soient premiers entre eux, les équations

$$\varphi_1(x, y_1) = 0, \quad \varphi_2(x, y_2) = 0, \quad \ldots, \quad \varphi_\omega(x, y_\omega) = 0$$

n'auront que la seule racine x commune ; donc on pourra exprimer x rationnellement par les coefficients de ces équations, et, par conséquent, en fonction rationnelle de $y_1, y_2, \ldots, y_\omega$. Ces dernières quantités étant connues, on aura ainsi l'une des racines de l'équation (1), et l'on en conclura ensuite toutes les autres

La résolution de l'équation (1) est donc ramenée à la recherche d'une racine de chacune des équations

$$\psi_1(y_1) = 0, \quad \psi_2(y_2) = 0, \quad \ldots, \quad \psi_\omega(y_\omega) = 0,$$

qui sont respectivement des degrés $m_1, m_2, \ldots, m_\omega$. En outre, ces équations ont la même propriété que la proposée, ainsi que nous l'avons établi précédemment ; on pourra donc leur appliquer la même méthode. Si l'on veut que ces équations soient le moins élevées possible, et si, en décomposant μ en facteurs premiers, on a

$$\mu = \varepsilon_1^{p_1} \varepsilon_2^{p_2} \ldots \varepsilon_\omega^{p_\omega},$$

il faudra prendre

$$m_1 = \varepsilon_1^{p_1}, \quad m_2 = \varepsilon_2^{p_2}, \quad \ldots, \quad m_\omega = \varepsilon_\omega^{p_\omega}.$$

Quant à la résolution de chacune des équations

$$\psi(y) = 0$$

de degré ε^p, elle se ramène à celle de P équations de degré ε, ainsi que nous l'avons démontré.

Des équations irréductibles dont deux racines x et x' sont liées par la relation linéaire $x' = \frac{ax+b}{a'x+b'}$, où a, b, a', b' sont des constantes données.

538. Soit

(1) $$f(x) = 0$$

une équation irréductible, et supposons qu'entre deux racines x et x' on ait la relation

(2) $$x' = \frac{ax+b}{a'x+b'} = \theta x,$$

où a, b, a', b' sont des constantes données. Les quantités comprises dans la série indéfinie

$$x, \quad \theta x, \quad \theta^2 x, \quad \theta^3 x, \quad \ldots$$

doivent être racines de l'équation (1), et nous savons que l'une des fonctions θx, $\theta^2 x$, ... est égale à x. Supposons

(3) $$\theta^\mu x = x.$$

Cette équation aura lieu identiquement, si l'on suppose que a, b, a', b' soient commensurables, ou, du moins, que ce soient des fonctions rationnelles des quantités regardées comme connues, et dont dépendent rationnellement les coefficients de l'équation proposée. Par conséquent, on aura ces formules obtenues au n° 463

(4) $$\left\{\begin{aligned} b' &= -\left(a - 2\cos\frac{\lambda\pi}{\mu}\right), \\ b &= -\frac{a^2 - 2a\cos\frac{\lambda\pi}{\mu} + 1}{a'}, \end{aligned}\right.$$

où λ désigne un nombre entier premier avec μ.

Dans le cas de $\mu = 2$, la condition (3) exige seulement que l'on ait

$$a + b' = 0;$$

on peut d'ailleurs supposer dans ce cas

$$ab' - ba' = \pm 1,$$

et alors on a

$$(5) \qquad \begin{cases} b' = -a, \\ b = -\dfrac{a^2 \pm 1}{a'}. \end{cases}$$

Le degré de l'équation (1) étant désigné par $n\mu$ et les $n\mu$ racines étant représentées par

$$\begin{array}{lllll} x, & \theta x, & \theta^2 x, & \ldots, & \theta^{\mu-1} x, \\ x_1, & \theta x_1, & \theta^2 x_1, & \ldots, & \theta^{\mu-1} x_1, \\ x_2, & \theta x_2, & \theta^2 x_2, & \ldots, & \theta^{\mu-1} x_2, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ x_{n-1}, & \theta x_{n-1}, & \theta^2 x_{n-1}, & \ldots, & \theta^{\mu-1} x_{n-1}, \end{array}$$

si l'on pose

$$(6) \qquad x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x = y,$$

y dépendra d'une équation

$$(7) \qquad F(y) = 0$$

de degré n, et dont les coefficients seront des fonctions rationnelles des quantités connues de l'équation (1) et de la fonction θ. L'équation (7) peut n'être pas résoluble algébriquement, mais les quantités

$$x, \quad \theta x, \quad \theta^2 x, \quad \ldots, \quad \theta^{\mu-1} x$$

dépendent d'une équation de degré μ dont les coefficients sont des fonctions rationnelles de y, et qui est, comme nous savons, résoluble. Dans le cas qui nous occupe, cette

dernière équation n'est autre que l'équation (6), et l'on voit, en conséquence, que l'équation proposée (1) doit résulter de l'élimination de y entre les deux équations (6) et (7); la seconde équation peut être considérée comme ayant pour premier membre un polynôme irréductible quelconque de degré n.

En d'autres termes, les équations que nous étudions peuvent être obtenues en multipliant un certain nombre n d'équations de la forme

$$x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x - y = 0,$$
$$x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x - y_1 = 0,$$
$$x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x - y_2 = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x - y_{n-1} = 0,$$

où $y, y_1, y_2, \ldots, y_{n-1}$ désignent les n racines d'une équation irréductible dont les coefficients sont des quantités entièrement arbitraires.

Il est évident qu'à l'équation (6) on peut substituer la suivante :

$$x \times \theta x \times \theta^2 x \times \ldots \times \theta^{\mu-1} x = y.$$

Des équations irréductibles à coefficients numériques dont plusieurs racines se développent en des fractions continues terminées par les mêmes quotients.

539. Nous avons fait connaître au n° 26 la forme des équations du deuxième degré dont les racines se développent en des fractions continues terminées par les mêmes quotients, et nous avons résolu ensuite (n° 512) la même question à l'égard des équations du troisième degré. Les considérations que nous avons développées

précédemment nous permettent de résoudre le problème plus général dont voici l'énoncé :

Quelles sont les équations irréductibles jouissant de la propriété que si l'on développe leurs racines réelles en fractions continues, par la méthode de Lagrange, deux ou plusieurs de ces fractions continues soient terminées par les mêmes quotients?

Pour que deux racines x' et x d'une équation se développent en des fractions continues terminées par les mêmes quotients, il faut et il suffit (n° 16) que l'on ait

$$x' = \frac{ax+b}{a'x+b'} = \theta x,$$

a, b, a', b' étant des entiers positifs ou négatifs liés par la relation

$$ab' - ba' = \pm 1;$$

en outre, pour que x et θx puissent représenter deux racines d'une équation irréductible, il faut qu'on puisse assigner un nombre entier μ, tel qu'on ait identiquement

$$\theta^\mu x = x;$$

si μ est > 2, cela exige, comme nous l'avons vu, qu'on ait

$$b' = -\left(a - 2\cos\frac{\lambda\pi}{\mu}\right),$$

$$b = -\frac{a^2 - 2a\cos\dfrac{\lambda\pi}{\mu} + 1}{a'};$$

λ étant un nombre entier premier avec μ, et, dans le cas de $\mu = 2$, on a

$$b' = -a,$$

$$b = -\frac{a^2 \pm 1}{a'}.$$

Or, puisque a, b, a', b' sont des nombres entiers, $2\cos\frac{\lambda\pi}{\mu}$ doit être un nombre entier, ce qui ne peut arriver que si μ est égal à 3, le cas de $\mu = 2$ étant réservé. On voit par là que la propriété que nous étudions ne peut se rencontrer que chez les équations irréductibles dont le degré a la forme $2n$ ou la forme $3n$. Nous examinerons successivement ces deux classes d'équations.

Si l'on suppose $\mu = 2$, on a

$$\theta x = \frac{ax - \frac{a^2 \pm 1}{a'}}{a'x - a}$$

et

$$\theta^2 x = x;$$

a désigne un nombre entier quelconque, et a' un diviseur de $a^2 \pm 1$. Si l'on prend pour $F(y)$ un polynôme irréductible quelconque de degré n, et qu'on élimine y entre les deux équations

$$x + \theta x = y, \quad F(y) = 0,$$

ou

$$x^2 - yx + \left(\frac{ay}{a'} - \frac{a^2 \pm 1}{a'^2}\right) = 0, \quad F(y) = 0,$$

on aura la forme générale des équations de degré $2n$ jouissant de cette propriété, que les $2n$ racines se partageront en n groupes tels que, dans chaque groupe de deux racines réelles, les fractions continues qui représentent ces racines seront terminées par les mêmes quotients.

Cette proposition peut être énoncée d'une autre manière :

Soient a un nombre entier quelconque, a' un diviseur quelconque de $a^2 + 1$, y une quantité réelle quelconque commensurable ou incommensurable; les deux racines

de l'équation

$$x^2 - yx + \left(\frac{ay}{a'} - \frac{a^2 \pm 1}{a'^2}\right) = 0$$

se développeront en des fractions continues terminées par les mêmes quotients, ce qui s'accorde avec le résultat obtenu au n° 26.

Supposons maintenant $\mu = 3$; on aura, en faisant $\lambda = 2$ (le cas de $\lambda = 1$ est identique à celui de $\lambda = 2$, on passe de l'un à l'autre en changeant les signes de a et de a'),

$$\theta x = \frac{ax - \dfrac{a^2 + a + 1}{a'}}{a'x - a + 1},$$

$$\theta^2 x = \frac{(a+1)x - \dfrac{a^2 + a + 1}{a'}}{a'x - a},$$

$$\theta^3 x = x;$$

a est un nombre entier quelconque, et a' un diviseur de $a^2 + a + 1$. Quelle que soit l'irrationnelle x, les fractions continues dans lesquelles se développent

$$x, \ \theta x, \ \theta^2 x$$

se termineront par les mêmes quotients. Si donc $F(y)$ désigne un polynôme irréductible quelconque de degré n, et qu'on élimine y entre les équations

$$x + \theta x + \theta^2 x = y, \quad F(y) = 0,$$

ou

$$x^3 - yx^2 + \left[\frac{(2a+1)y}{a'} - \frac{3(a^2 + a + 1)}{a'^2}\right]x$$
$$- \left[\frac{a(a+1)y}{a'^2} - \frac{(2a+1)(a^2 + a + 1)}{a'^3}\right] = 0,$$

$$F(y) = 0,$$

on obtiendra l'expression générale des équations de degré $3n$ qui jouissent de la propriété, que les $3n$ racines se partageront en n groupes tels que, dans chaque groupe de trois racines réelles, les fractions continues dans lesquelles se développent ces racines seront terminées par les mêmes quotients.

On voit, en particulier, que les équations du troisième degré qui ont cette propriété sont comprises dans la forme générale suivante :

$$x^3 - yx^2 + \left[\frac{(2a+1)y}{a'} - \frac{3(a^2+a+1)}{a'^2}\right]x$$
$$- \left[\frac{a(a+1)y}{a'^2} - \frac{(2a+1)(a^2+a+1)}{a'^2}\right] = 0,$$

où a désigne un entier quelconque, a' un diviseur quelconque de a^2+a+1, et y une quantité quelconque, commensurable ou incommensurable. Ce résultat s'accorde avec celui que nous avons obtenu au n° 512.

540. Les équations du troisième degré qui proviennent de la division du cercle en sept ou en neuf parties égales, celle du quatrième degré qui provient de la division en quinze parties égales, jouissent de la propriété remarquable qu'on vient d'étudier.

La division du cercle en sept parties égales conduit à l'équation

$$x^3 + x^2 - 2x - 1 = 0,$$

et si l'on représente par x la racine positive par $-x_1$ et $-x_2$ les deux racines négatives, on a

$$x_1 = \frac{1}{1+x}, \quad x_2 = 1 + \frac{1}{x};$$

la racine x est comprise entre 1 et 2; on aura, par con-

séquent, des résultats de cette forme :

$$x = 1 + \cfrac{1}{\alpha + \cfrac{1}{\beta + \ldots}}, \qquad x_1 = \cfrac{1}{2 + \cfrac{1}{\alpha + \cfrac{1}{\beta + \ldots}}},$$

$$x_2 = 1 \ \cfrac{1}{1 + \cfrac{1}{\alpha + \cfrac{1}{\beta + \ldots}}}.$$

La division du cercle en neuf parties égales conduit à l'équation

$$x^3 - 3x + 1 = 0.$$

Si l'on désigne par $-x$ la racine négative, laquelle est comprise entre -1 et -2, par x_1 et x_2 les deux racines positives, on a

$$x_1 = \frac{1}{1+x}, \quad x_2 = 1 + \frac{1}{x},$$

ce qui conduit aux mêmes résultats que le cas précédent.

Enfin, l'équation du quatrième degré dont dépend la division du cercle en quinze parties égales est

$$x^4 - x^3 - 4x^2 + 4x + 1 = 0.$$

Si x et x_1 désignent les deux racines positives, $-x'$ et $-x'_1$ les deux négatives, on a

$$x = \frac{x'+2}{x'+1} = 1 + \frac{1}{1+x'},$$

$$x_1 = \frac{x'_1+2}{x'_1+1} = 1 + \frac{1}{1+x'_1},$$

Des deux quantités x' et x'_1 l'une est comprise entre 0 et 1, l'autre entre 1 et 2; on aura donc des résultats de

cette forme

$$x' = \cfrac{1}{\alpha + \cfrac{1}{6 + \dotsb}}, \qquad x = 1 + \cfrac{1}{1 + \cfrac{1}{\alpha + \cfrac{1}{6 + \dotsb}}},$$

$$x'_1 = 1 + \cfrac{1}{\alpha' + \cfrac{1}{6' + \dotsb}}, \qquad x_1 = 1 + \cfrac{1}{2 + \cfrac{1}{\alpha' + \cfrac{1}{6' + \dotsb}}}.$$

L'équation que nous considérons résulte de l'élimination de y entre

$$x + \frac{x-2}{x-1} = y, \quad y^2 - y - 1 = 0.$$

Des équations dont toutes les racines sont exprimables rationnellement par l'une d'entre elles.

541. Nous avons étudié précédemment un cas étendu des équations dont les racines sont toutes exprimables rationnellement par l'une d'entre elles; savoir le cas où, l'équation proposée étant du degré μ, les racines peuvent être représentées par

$$x,\ \theta x,\ \theta^2 x,\ \ldots,\ \theta^{\mu-1} x;$$

alors ces racines sont exprimables par des radicaux.

Il existe un autre cas de résolubilité; Abel a effectivement démontré le théorème suivant :

THÉORÈME. — *Soit* $\chi(x) = 0$ *une équation algébrique quelconque, dont toutes les racines peuvent être exprimées rationnellement par l'une d'entre elles que nous désignerons par* x. *Soient* θx *et* $\theta_1 x$ *deux autres racines quelconques; l'équation proposée sera résoluble algé-*

briquement si l'on a

$$\theta\theta_1 x = \theta_1 \theta x.$$

En effet, si l'équation proposée

$$(1) \qquad \chi(x) = 0$$

n'est pas irréductible, soit

$$(2) \qquad f(x) = 0$$

l'équation irréductible de degré μ dont dépend la racine x, le polynôme $f(x)$ sera un diviseur rationnel de $\chi(x)$.

Soit θx une racine de l'équation (2), autre que x; les racines de cette équation pourront être représentées par

$$\begin{array}{lllll} x, & \theta x, & \theta^2 x, & \ldots, & \theta^{n-1} x, \\ x_1, & \theta x_1, & \theta^2 x_1, & \ldots, & \theta^{n-1} x_1, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{m-1}, & \theta x_{m-1}, & \ldots\ldots, & & \theta^{n-1} x_{m-1}; \end{array}$$

on aura

$$\mu = mn,$$

et, si l'on représente par

$$(3) \qquad x^n + A^{(1)} x^{n-1} + A^{(2)} x^{n-2} + \ldots + A^{(n-1)} x + A^{(n)} = 0$$

l'équation qui a pour racines

$$x, \quad \theta x, \quad \theta^2 x, \quad \ldots, \quad \theta^{n-1} x,$$

les coefficients $A^{(1)}, A^{(2)}, \ldots, A^{(n)}$ sont, comme on l'a vu, exprimables rationnellement en fonction d'une quantité y qui dépend d'une équation de degré m,

$$(4) \qquad y^m + P^{(1)} y^{m-1} + P^{(2)} y^{m-2} + \ldots + P^{(m-1)} y + P^{(m)} = 0,$$

dont les coefficients sont des fonctions rationnelles des quantités connues.

Cette équation (4) est irréductible, car si le contraire

avait lieu, y serait racine d'une équation irréductible

$$(5)\qquad \varphi(y)=0,$$

d'un degré m' inférieur à m, et l'élimination de y entre les équations (3) et (5) conduirait à une équation

$$\psi(x)=0,$$

de degré $m'n<\mu$; ce qui est impossible, car l'équation (2) du degré μ est, par hypothèse, irréductible.

Cela posé, la résolution de l'équation (2) est ramenée à celle des équations (3) et (4); nous savons que l'équation (3) est résoluble, et nous allons démontrer que l'équation (4) possède la même propriété que l'équation (2).

La quantité y est une fonction rationnelle et symétrique quelconque des racines $x, \theta x, \ldots, \theta^{n-1}x$, et si l'on désigne par

$$y,\ y_1,\ y_2,\ \ldots,\ y_{m-1}$$

les m racines de l'équation (4), on pourra poser

$$\begin{aligned}
y &= \mathfrak{F}(x,\ \theta x,\ \theta^2 x,\ \ldots,\ \theta^{n-1}x),\\
y_1 &= \mathfrak{F}(x_1,\ \theta x_1,\ \theta^2 x_1,\ \ldots,\ \theta^{n-1}x_1),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
y_{m-1} &= \mathfrak{F}(x_{m-1},\ \theta x_{m-1},\ \ldots\ldots,\ \theta^{n-1}x_{m-1}),
\end{aligned}$$

$\mathfrak{F}$ désignant une fonction symétrique et rationnelle. D'ailleurs $x_1, x_2, \ldots, x_{m-1}$ sont, par hypothèse, des fonctions rationnelles de la racine x; si donc on fait

$$x_1=\theta_1 x,\quad x_2=\theta_2 x,\quad \ldots,\quad x_{m-1}=\theta_{m-1}x,$$

on aura, pour les valeurs $1, 2, \ldots, m-1$ de l'indice i,

$$y_i=\mathfrak{F}(\theta_i x,\ \theta\theta_i x,\ \theta^2\theta_i x,\ \ldots,\ \theta^{n-1}\theta_i x).$$

Enfin, d'après l'énoncé du théorème, les fonctions θ et θ_i sont telles, que l'on a

$$\theta\theta_i x=\theta_i\theta x;$$

il en résulte

$$\theta^j\theta_i x = \theta^{j-1}\theta_i\theta x = \theta^{j-2}\theta_i\theta^2 x = \ldots = \theta_i\theta^j x,$$

et, en conséquence, on peut écrire,

$$y_i = \mathfrak{F}(\theta_i x,\ \theta_i\theta x,\ \theta_i\theta^2 x,\ \ldots,\ \theta_i\theta^{n-1}x),$$

ce qui montre que y_i est une fonction rationnelle et symétrique des racines

$$x,\ \theta x,\ \theta^2 x,\ \ldots,\ \theta^{n-1}x.$$

On peut conclure de là (n° 531) que $y_1, y_2, \ldots, y_{m-1}$ sont exprimables en fonction rationnelle de y.

Soient maintenant λy et $\lambda_1 y$ deux racines quelconques de l'équation (4) autres que y, on pourra poser

$$(6)\qquad \left\{\begin{aligned} y &= F(x),\\ \lambda\, y &= F(\theta_i x),\\ \lambda_1 y &= F(\theta_j x),\end{aligned}\right.$$

et il en résultera

$$\lambda\, F(x) = F(\theta_i x),$$
$$\lambda_1 F(x) = F(\theta_j x).$$

Or, x étant racine d'une équation irréductible, les équations précédentes subsisteront si l'on remplace x par $\theta_j x$ dans la première, et par $\theta_i x$ dans la seconde; on aura donc

$$\lambda\, F(\theta_j x) = F(\theta_i\theta_j x),$$
$$\lambda_1 F(\theta_i x) = F(\theta_j\theta_i x),$$

d'où

$$\lambda F(\theta_j x) = \lambda_1 F(\theta_i x),$$

puisque $\theta_i\theta_j x = \theta_j\theta_i x$. Les équations (6) permettent de donner à la formule précédente la forme

$$\lambda\lambda_1 y = \lambda_1\lambda y,$$

d'où il suit que l'équation (4) a bien la même propriété que l'équation (1).

On pourra donc, en continuant d'appliquer le même procédé, ramener la résolution de l'équation proposée à celle de plusieurs équations qui seront toutes résolubles algébriquement, et dont les degrés auront pour produit le degré μ de l'équation (2).

Corollaire. — *Si l'équation $f(x)=0$ a la propriété contenue dans l'énoncé du théorème précédent, et que, son degré μ étant décomposé en facteurs premiers, on ait*

$$\mu = \varepsilon_1^{p_1}\varepsilon_2^{p_2}\ldots\varepsilon_\omega^{p_\omega},$$

la résolution de $f(x)=0$ peut être ramenée à celle de p_1 équations du degré ε_1, de p_2 équations du degré $\varepsilon_2, \ldots,$ de p_ω équations du degré ε_ω, et toutes ces équations, dont les coefficients sont rationnels, sont résolubles algébriquement.

Résolution algébrique des équations binômes.

542. L'équation binôme

$$(1) \qquad z^m - A = 0$$

se réduit à

$$(2) \qquad x^m - 1 = 0,$$

si l'on pose $z = x\sqrt[m]{A}$, et nous avons vu dans le Chapitre V de la Section I que la recherche des racines de l'équation (2), dans le cas où m est un nombre composé, se ramène à la résolution d'équations binômes de degrés premiers.

Supposons donc que l'exposant m soit un nombre premier; l'équation (2) admet la racine 1, et, en supprimant cette racine, on obtient l'équation

$$(3) \qquad x^{m-1} + x^{m-2} + x^{m-3} + \ldots + x^2 + x + 1 = 0,$$

qui est irréductible, ainsi que nous l'avons établi au n° 110.

L'équation (3) appartient à la classe des équations que nous avons nommées *abéliennes*, et ses racines peuvent, en conséquence, s'exprimer par des fonctions algébriques dans lesquelles les radicaux ont pour indices les facteurs premiers de $m-1$. Effectivement, si r est une racine de l'équation (3), cette équation aura pour racines

$$r,\ r^2,\ r^3,\ \ldots,\ r^{m-1};$$

on a d'ailleurs

$$r^m = 1,$$

et, si l'on désigne par a une racine primitive pour le nombre premier m, les puissances

$$a^0,\ a^1,\ a^2,\ a^3,\ \ldots,\ a^{m-2}$$

seront respectivement congrues, suivant le module m, et abstraction faite de l'ordre, aux nombres

$$1,\ 2,\ 3,\ \ldots,\ m-1;$$

donc les racines de l'équation (3) peuvent être représentées par

$$(4)\qquad r,\ r^a,\ r^{a^2},\ r^{a^3},\ \ldots,\ r^{a^{m-2}},$$

en sorte que chacune d'elles s'obtient en élevant la précédente à la puissance a; et la même chose a lieu encore, à cause de

$$a^{m-1} \equiv 1 \pmod{m},$$

si l'on range en cercle ces m racines et que l'on considère successivement chacune d'elles comme étant la première.

D'après cela, si x désigne l'une quelconque des racines (4), et que l'on fasse

$$x^a = \theta x,$$

les $m-1$ racines dont il s'agit seront représentées par

$$x,\ \theta x,\ \theta^2 x\ \ldots,\ \theta^{m-2} x,$$

et l'on aura

$$\theta^{m-1} x = x.$$

C'est sur cette propriété que Gauss a fondé sa méthode pour la résolution de l'équation (3), méthode qu'Abel a généralisée ensuite comme nous l'avons expliqué.

On peut appliquer à l'équation (2) la méthode du n° 532, et l'on a ainsi l'expression des racines, savoir:

$$x = \frac{-A + \sqrt[m-1]{v_1} + \sqrt[m-1]{v_2} + \ldots + \sqrt[m-1]{v_{m-2}}}{m-1},$$

dans laquelle $v_1, v_2, \ldots, v_{m-2}$ ne contiennent d'autres irrationnelles que les racines de l'équation

$$x^{m-1} = 1.$$

Mais, comme $m-1$ est un nombre composé, on obtiendra une solution plus simple en faisant usage des méthodes exposées aux n°s 535 et 537.

Enfin, comme l'équation (3) appartient à la classe des équations réciproques, on peut commencer par lui appliquer la méthode d'abaissement qui se rapporte à ces équations; on obtient alors une équation du degré $\frac{m-1}{2}$ dont toutes les racines sont réelles et qui conserve le caractère d'équation abélienne : c'est ce que nous allons développer présentement.

Résolution algébrique des équations dont dépend la division de la circonférence du cercle en un nombre premier de parties égales.

543. Le problème de la division du cercle en un nombre m quelconque de parties égales se ramène à la

résolution de l'équation binôme

(1) $$z^m - 1 = 0;$$

car, si l'on fait

$$\frac{2\pi}{m} = a,$$

on obtiendra les m racines de l'équation précédente, en donnant à k les m valeurs

$$0,\ 1,\ 2,\ 3,\ \ldots,\ (m-1)$$

dans la formule

$$z = \cos ka + \sqrt{-1}\sin ka;$$

on connaîtra donc $\cos ka$ et $\sin ka$ lorsque l'équation binôme (1) sera résolue algébriquement.

Si m est un nombre impair $2\mu+1$, il vient, en divisant l'équation (1) par $z-1$, et en posant ensuite $z+\frac{1}{z}=x$,

(2) $$\left\{\begin{aligned} & x^\mu + x^{\mu-1} - (\mu-1)x^{\mu-2} - (\mu-2)x^{\mu-3} \\ & \quad + \frac{(\mu-2)(\mu-3)}{1.2}x^{\mu-4} + \frac{(\mu-3)(\mu-4)}{1.2}x^{\mu-5} - \ldots = 0. \end{aligned}\right.$$

C'est de cette équation (2) que dépend directement la division du cercle en $2\mu+1$ parties égales. Ses μ racines sont représentées par la formule

$$x = 2\cos\frac{2k\pi}{2\mu+1} = 2\cos ka,$$

dans laquelle on doit donner à k les μ valeurs

$$1,\ 2,\ 3,\ \ldots,\ \mu,$$

ou des valeurs qui ne diffèrent de celles-là que par des multiples de $2\mu+1$.

Nous venons de rappeler que, si m ou $2\mu+1$ est un nombre composé, la résolution de l'équation (1) se ramène à la résolution d'autres équations de la même forme, et qui ont pour degrés respectifs les nombres premiers ou les puissances de nombres premiers qui divisent m. Dès lors, la même chose peut se dire de l'équation (2), et l'on peut se borner à considérer le cas où $m=2\mu+1$ est un nombre premier ou une puissance d'un nombre premier. Lorsque m est premier, la division de la circonférence en m parties égales exige seulement la résolution de plusieurs équations qui ont respectivement pour degrés les facteurs premiers égaux ou inégaux dans lesquels se décompose le nombre $m-1$. Mais, lorsque m est une puissance p^i d'un nombre premier p, la division de la circonférence en m parties égales exige d'abord la division en p parties égales, et, en outre, la résolution de $i-1$ équations de degré p. Chacune de ces $i-1$ équations de degré p est résoluble algébriquement; cela résulte soit de la formule de Moivre, soit des considérations développées dans la Section I.

Il faut d'ailleurs remarquer que, quel que soit μ, l'équation (2) appartient à la classe des équations dont nous nous sommes occupés au n° 541. Car si l'on fait

$$x=2\cos a,\quad \theta x=2\cos ia,\quad \theta_1 x=2\cos ja,$$

on a évidemment

$$\theta\theta_1 x=\theta_1\theta x=2\cos ija.$$

544. Supposons $2\mu+1$ premier, et soit n une racine primitive pour ce nombre premier; je dis que les μ racines de l'équation (2) seront

$$(3)\qquad 2\cos a,\quad 2\cos na,\quad 2\cos n^2 a,\quad \ldots,\quad 2\cos n^{\mu-1} a.$$

Il est évident que chacune de ces μ quantités satisfait à

l'équation (2); il suffit donc de démontrer qu'elles sont toutes distinctes. Supposons, s'il est possible, que deux de ces quantités soient égales, et que l'on ait

$$2\cos n^p a = 2\cos n^q a,$$

p et q étant $< \mu$; on aura

$$n^p a \pm n^q a = 2\lambda\pi,$$

λ désignant un nombre entier. Mais $a = \dfrac{2\pi}{2\mu+1}$, donc

$$\frac{n^q(n^{p-q} \pm 1)}{2\mu+1}$$

est un nombre entier; d'ailleurs $2\mu+1$ est un nombre premier, et n est inférieur à $2\mu+1$; il s'ensuit que $2\mu+1$ divise l'un des deux nombres $n^{p-q}+1$ ou $n^{p-q}-1$; par conséquent il divise le produit

$$n^{2p-2q}-1$$

de ces deux nombres; or cela est impossible, car $2p-2q$ est $< 2\mu$, et n désigne une racine primitive de $2\mu+1$. Donc les quantités (3) sont bien toutes les racines de l'équation (2).

Si maintenant on fait

$$x = 2\cos a, \quad \theta x = 2\cos na,$$

on aura

$$\theta^2 x = 2\cos n^2 a, \quad \theta^3 x = 2\cos n^3 a, \quad \ldots, \quad \theta^{\mu-1} x = 2\cos n^{\mu-1} a,$$

et les racines de l'équation (2) seront représentées par

$$x, \quad \theta x, \quad \theta^2 x, \quad \ldots, \quad \theta^{\mu-1} x;$$

on a, en outre, $\theta^\mu x = x$; car, n étant une racine primitive de $2\mu+1$, on a $n^\mu \equiv -1 \pmod{2\mu+1}$; enfin θx est une fonction rationnelle de x, car $\cos na$ est exprimable

rationnellement en fonction de $\cos a$. On voit donc que l'équation (2) est comprise dans la classe des équations abéliennes, et l'on pourra la résoudre par les méthodes que nous avons exposées.

Ici la fonction rationnelle θx a pour valeur (n° 109)

$$\theta x = x^n - n x^{n-2} + \frac{n(n-3)}{1.2} x^{n-4} - \frac{n(n-4)(n-5)}{1.2.3} x^{n-6} + \ldots.$$

En appliquant à l'équation (2) les théorèmes des n°s 534 et 535, on obtient les énoncés suivants :

1° *Si* $\mu = m_1 m_2 \ldots m_\omega$, *on peut diviser la circonférence entière du cercle en* $2\mu + 1$ *parties égales à l'aide de* ω *équations des degrés* $m_1, m_2, \ldots, m_\omega$ *respectivement. Si les nombres* $m_1, m_2, \ldots, m_\omega$ *sont premiers entre eux, les coefficients de ces équations seront des nombres rationnels.*

2° *Si* $\mu = 2^\omega$, *on pourra diviser la circonférence du cercle en* $2\mu + 1$ *parties égales, à l'aide de* ω *racines carrées. En d'autres termes, si* $2\mu + 1$ *est un nombre premier, et* $\mu = 2^\omega$, *on pourra diviser la circonférence du cercle en* $2\mu + 1$ *parties égales, avec la règle et le compas.*

3° *Pour diviser la circonférence du cercle en* $2\mu + 1$ *parties égales, il suffit de diviser la circonférence entière en* 2μ *parties égales, de diviser un arc, qu'on peut construire ensuite en* 2μ *parties égales, et d'extraire la racine carrée d'une seule quantité.*

545. Le dernier théorème est dû à Gauss. Cet illustre géomètre a prouvé, en outre, que la quantité dont il faut extraire la racine carrée est simplement le nombre entier $2\mu + 1$. Voici comment Abel le démontre.

Cette quantité, que nous désignerons par ρ, est (n° 534)

la valeur numérique du produit

$$+\alpha\theta x+\alpha^2\theta^2 x+\ldots+\alpha^{\mu-1}\theta^{\mu-1}x)\,(x+\alpha^{\mu-1}\theta x+\alpha^{\mu-2}\theta^2 x+\ldots+\alpha\theta^{\mu-1}x),$$

où

$$\alpha=\cos\frac{2\pi}{\mu}+\sqrt{-1}\sin\frac{2\pi}{\mu}.$$

On a donc

$$\begin{aligned}\pm\rho=4\,&(\cos a+\alpha\cos na+\alpha^2\cos n^2 a+\ldots+\alpha^{\mu-1}\cos n^{\mu-1}a)\\ &\times(\cos a+\alpha^{\mu-1}\cos na+\alpha^{\mu-2}\cos n^2 a+\ldots+\alpha\cos n^{\mu-1}a).\end{aligned}$$

En développant ce produit, on obtient un résultat de la forme

$$\pm\rho=t_0+t_1\alpha+t_2\alpha^2+\ldots+t_{\mu-1}\alpha^{\mu-1},$$

et l'on trouve facilement

$$\begin{aligned}=4\,&(\cos a\cos n^m a+\cos na\cos n^{m+1}a+\ldots+\cos n^{\mu-1-m}a\cos n^{\mu-1}a)\\ +4\,&(\cos n^{\mu-m}a\cos a+\cos n^{\mu-m+1}a\cos na+\ldots+\cos n^{\mu-1}a\cos n^{m-1}a).\end{aligned}$$

Au moyen de la formule

$$\cos n^p a\cos n^{m+p}a=\frac{1}{2}\cos(n^{m+p}a+n^p a)+\frac{1}{2}\cos(n^{m+p}a-n^p a),$$

on donnera à t_m la forme

$$\begin{aligned}t_m=2&\left[\begin{matrix}\cos(n^m+1)a+\cos(n^m+1)na+\cos(n^m+1)n^2a+\ldots\\ +\cos(n^m+1)n^{\mu-1}a\end{matrix}\right]\\ +2&\left[\begin{matrix}\cos(n^m-1)a+\cos(n^m-1)na+\cos(n^m-1)n^2a+\ldots\\ +\cos(n^m-1)n^{\mu-1}a\end{matrix}\right],\end{aligned}$$

ou, en faisant $(n^m+1)a=a'$, $(n^m-1)a=a''$,

$$\begin{aligned}t_m&=2\cos a'+\theta\,2\cos a'+\theta^2\,2\cos a'+\ldots+\theta^{\mu-1}\,2\cos a'\\ &+2\cos a''+\theta\,2\cos a''+\theta^2\,2\cos a''+\ldots+\theta^{\mu-1}\,2\cos a''.\end{aligned}$$

Cela posé, supposons d'abord que m ne soit pas nul, $2\cos a'$ et $2\cos a''$ sont des racines de l'équation (2); donc

$$2\cos a' = \theta^\delta x \quad \text{et} \quad 2\cos a'' = \theta^\iota x,$$

et l'on a, en conséquence,

$$t_m = (\theta^\delta x + \theta^{\delta+1} x + \ldots + \theta^{\mu-1} x + x + \theta x + \ldots + \theta^{\delta-1} x)$$
$$+ (\theta^\iota x + \theta^{\iota+1} x + \ldots + \theta^{\mu-1} x + x + \theta x + \ldots + \theta^{\iota-1} x),$$

ou

$$t_m = 2(x + \theta x + \theta^2 x + \ldots + \theta^{\mu-1} x);$$

d'où il résulte que t_m est double de la somme des racines de l'équation (2), laquelle est égale à -1; on a donc

$$t_m = -2.$$

Supposons maintenant $m = 0$, on aura

$$t_0 = 2(\cos 2a + \cos 2na + \cos 2n^2 a + \ldots + \cos 2n^{\mu-1} a) + 2\mu.$$

Or $2\cos 2a$ est racine de l'équation (2); donc, en faisant

$$2\cos 2a = \theta^\delta x,$$

on aura

$$t_0 = (\theta^\delta x + \theta^{\delta+1} x + \ldots + \theta^{\mu-1} x + x + \theta x + \ldots + \theta^{\delta-1} x) + 2\mu,$$

et, par conséquent,

$$t_0 = 2\mu - 1.$$

D'après cela, la valeur de $\pm \rho$ sera

$$\pm \rho = 2\mu - 1 - 2(\alpha + \alpha^2 + \ldots + \alpha^{\mu-1}).$$

D'ailleurs

$$\alpha + \alpha^2 + \ldots + \alpha^{\mu-1} = -1,$$

donc

$$\pm \rho = 2\mu + 1.$$

Ce qu'il fallait démontrer.

Division de la circonférence en dix-sept parties égales.

546. Si l'on fait $2\mu+1=17$ ou $\mu=8$, l'équation (2) du numéro précédent devient

(1) $x^8+x^7-7x^6-6x^5+15x^4-10x^3-10x^2-4x+1=0,$

et ses racines, comprises dans la formule

$$x=2\cos\frac{2k\pi}{17},$$

peuvent être représentées par

(2) $x,\ \theta x,\ \theta^2 x,\ \theta^3 x,\ \theta^4 x,\ \theta^5 x,\ \theta^6 x,\ \theta^7 x.$

La plus petite racine primitive de 17 est 3 (n° 316), et les résidus par rapport à 17 des puissances

$$3^0,\ 3^1,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\ 3^6,\ 3^7$$

sont

$$1,\ 3,\ 9,\ 10,\ 13,\ 5,\ 15,\ 11;$$

si donc on pose, pour abréger,

$$a=\frac{2\pi}{17},$$

les quantités (2) seront

$$\begin{array}{llll} 2\cos a, & 2\cos 3a, & 2\cos 9a, & 2\cos 10a,\\ 2\cos 13a, & 2\cos 5a, & 2\cos 15a, & 2\cos 11a; \end{array}$$

ou, à cause de $\cos(17-m)a=\cos ma$,

$$\begin{array}{llll} 2\cos a, & 2\cos 3a, & 2\cos 8a, & 2\cos 7a,\\ 2\cos 4a, & 2\cos 5a, & 2\cos 2a, & 2\cos 6a. \end{array}$$

Pour appliquer la méthode générale, il faut commencer

par calculer une fonction rationnelle et symétrique y des quantités

$$2\cos a,\quad 2\cos 8a,\quad 2\cos 4a,\quad 2\cos 2a.$$

Posons donc

$$y = 2\cos a + 2\cos 8a + 2\cos 4a + 2\cos 2a;$$

y dépendra d'une équation du deuxième degré, dont les deux racines seront

$$(3)\qquad y = 2\cos a \quad + 2\cos 8a + 2\cos 4a + 2\cos 2a,$$
$$(4)\qquad y_1 = 2\cos 3a + 2\cos 7a + 2\cos 5a + 2\cos 6a.$$

Cette équation s'obtient bien facilement; car on a d'abord, par l'équation (1),

$$(5)\qquad y + y_1 = -1;$$

ensuite, en multipliant y par y_1, transformant les produits de cosinus en sommes à l'aide des formules connues, et ayant égard à l'équation identique

$$\cos(17 - m)a = \cos ma,$$

on trouve

$$yy_1 = 4(2\cos a + 2\cos 2a + 2\cos 3a + 2\cos 4a$$
$$+ 2\cos 5a + 2\cos 6a + 2\cos 7a + 2\cos 8a),$$

et, à cause de l'équation (1),

$$(6)\qquad yy_1 = -4.$$

L'équation en y sera donc

$$(7)\qquad y^2 + y - 4 = 0,$$

et l'on peut considérer comme connues ses deux racines y et y_1.

Maintenant les quantités

$$2\cos a,\quad 2\cos 8a,\quad 2\cos 4a,\quad 2\cos 2a,$$

sont les racines d'une équation du quatrième degré dont les coefficients sont des fonctions rationnelles de y, et sur laquelle nous allons raisonner comme nous l'avons fait sur la proposée. Il faut, conformément à la méthode générale, chercher d'abord une fonction rationnelle et symétrique z des quantités

$$2\cos a, \quad 2\cos 4a.$$

Posons donc

$$z = 2\cos a + 2\cos 4a,$$

l'équation en z sera du deuxième degré, et elle aura pour racines

$$(8) \qquad z = 2\cos a + 2\cos 4a,$$

$$(9) \qquad z_1 = 2\cos 8a + 2\cos 2a.$$

On a d'abord

$$(10) \qquad z + z_1 = y,$$

et, en multipliant z par z_1, on trouve, après avoir remplacé les produits de cosinus par des sommes,

$$zz_1 = (2\cos a + 2\cos 2a + 2\cos 3a + 2\cos 4a + 2\cos 5a + 2\cos 6a + 2\cot 7a + 2\cos 8a),$$

ou, puisque la somme des racines de l'équation (1) est -1,

$$(11) \qquad zz_1 = -1;$$

l'équation en z sera donc

$$(12) \qquad z^2 - yz - 1 = 0.$$

Enfin il ne reste plus qu'à former l'équation du deuxième degré dont les racines sont

$$2\cos a, \quad 2\cos 4a,$$

et dont les coefficients peuvent s'exprimer en fonction

rationnelle de y et de z. Mais on peut simplifier ici l'application de la méthode générale.

Considérons l'équation du quatrième degré, dont les racines

$$2\cos 3a,\quad 2\cos 7a,\quad 2\cos 5a,\quad 2\cos 6a$$

ont pour somme y_1, et opérons comme nous l'avons fait à l'égard de l'équation qui a pour racines les quantités dont la somme est y. On formera une équation du deuxième degré ayant pour racines

$$(13)\qquad u = 2\cos 3a + 2\cos 5a,$$

$$(14)\qquad u_1 = 2\cos 7a + 2\cos 6a,$$

et, en opérant comme précédemment, on trouvera

$$(15)\qquad u + u_1 = y_1,$$

$$(16)\qquad uu_1 = -1;$$

cette équation en u sera donc

$$(17)\qquad u^2 - y_1 u - 1 = 0,$$

en sorte que les quantités u et u_1 sont connues, ainsi que z et z_1.

Cela posé, faisons

$$(18)\qquad x = 2\cos a,$$

$$(19)\qquad x_1 = 2\cos 4a,$$

on aura d'abord

$$(20)\qquad x + x_1 = z,$$

et ensuite

$$xx_1 = 4\cos a\cos 4a = 2\cos 3a + 2\cos 5a$$

ou

$$(21)\qquad xx_1 = u;$$

x et x_1 seront donc racines de l'équation

$$(22)\qquad x^2 - zx + u = 0.$$

La résolution de l'équation (1) est ainsi ramenée à celle des équations du deuxième degré (7), (12), (17) et (22); le problème est donc résolu. Nous allons chercher maintenant à déduire de l'analyse précédente une construction géométrique, pour effectuer la division de la circonférence en dix-sept parties égales.

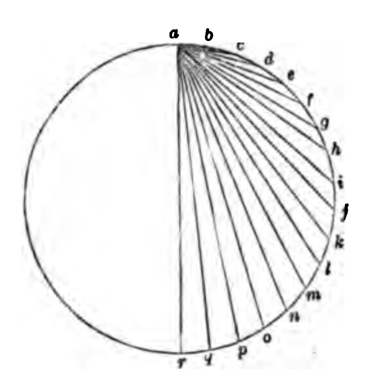
Construction géométrique.

547. Quand on se propose, dans la Géométrie élémentaire, d'inscrire dans un cercle les polygones réguliers de trois et de cinq côtés, on commence par inscrire ceux de six et dix côtés. De même, nous commencerons ici par inscrire le polygone régulier de trente-quatre côtés, celui de dix-sept côtés s'en déduira immédiatement.

Soit une demi-circonférence partagée en dix-sept parties égales aux points

$$a,\ b,\ c,\ d,\ e,\ f,\ g,\ h,\ i,\ j,\ k,\ l,\ m,\ n,\ o,\ p,\ q,\ r;$$

la corde ab sera le côté du polygone régulier inscrit de



trente-quatre côtés, et les cordes ad, af, ah, aj, al, an, ap, diagonales de ce polygone, seront les côtés des poly-

gones réguliers *étoilés* de trente-quatre côtés que l'on peut inscrire dans la circonférence.

En prenant le rayon pour unité et en faisant, comme précédemment,

$$a=\frac{2\pi}{17},$$

on aura

$$ab=2\sin\frac{\pi}{34}=+2\cos4a,$$
$$ad=2\sin\frac{3\pi}{34}=-2\cos5a,$$
$$af=2\sin\frac{5\pi}{34}=+2\cos3a,$$
$$ah=2\sin\frac{7\pi}{34}=-2\cos6a,$$
$$aj=2\sin\frac{9\pi}{34}=+2\cos2a,$$
$$al=2\sin\frac{11\pi}{34}=-2\cos7a,$$
$$an=2\sin\frac{13\pi}{34}=+2\cos a,$$
$$ap=2\sin\frac{15\pi}{34}=-2\cos8a.$$

Conservons toutes les notations du numéro précédent: les équations (3) et (4) nous donnent

$$y=an-ap+ab+aj,$$
$$y_1=af-al-ad-ah.$$

On voit que y_1 est négatif, car af est $<al$; par suite, y est positif, puisque $yy_1=-1$. Faisant donc $y_1=-y'$, les équations (5) et (6) deviennent

$$y'-y=1,$$
$$yy'=4,$$

les équations (8) et (9) nous donnent

$$z = an + ab,$$
$$z_1 = -ap + aj;$$

z_1 est négatif, car ap est $> aj$, et z est positif. Les équations (10) et (11) deviennent, en faisant $z_1 = -z'$,

$$z - z' = y,$$
$$zz' = 1.$$

Pareillement, les équations (13) et (14) donnent

$$u = af - ad,$$
$$u_1 = -al - ah;$$

u_1 est donc négatif, et u positif. Faisant $u_1 = -u'$, on aura, par les équations (15) et (16),

$$u' - u = y',$$
$$uu' = 1;$$

enfin les équations (18) et (19) donnent

$$x = an,$$
$$x_1 = ab,$$

en sorte que x et x_1 sont positifs, et les équations (20) et (21) conservent leur forme

$$x + x_1 = z,$$
$$xx_1 = u.$$

Le côté de notre polygone de trente-quatre côtés est x_1, et, pour le construire, on voit qu'il suffit :

1° De construire deux lignes y et y' telles, que

$$y' - y = 1, \quad yy' = 4;$$

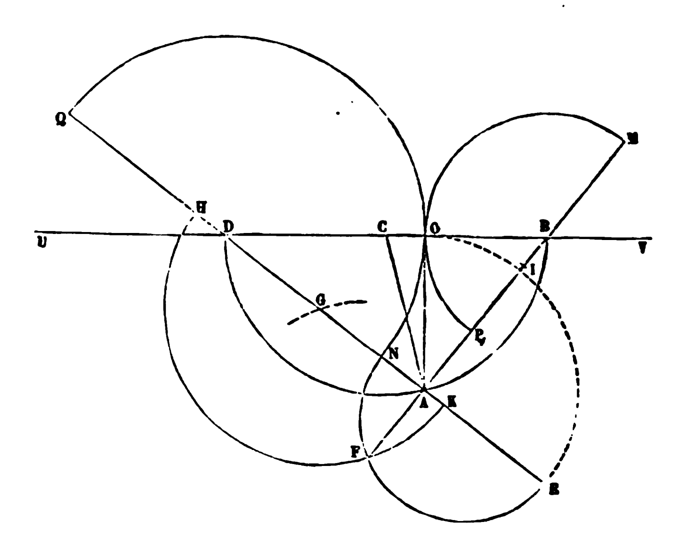
2° De construire quatre lignes z, z', u, u' telles, que

$$z - z' = y, \quad zz' = 1,$$
$$u' - u = y', \quad uu' = 1;$$

3° De construire deux lignes x et x_1 telles, que

$$x + x_1 = z, \quad xx_1 = u.$$

Construction. — 1° En un point O d'une ligne indé-



finie UV, élevons une perpendiculaire OA égale au rayon du cercle, c'est-à-dire égale à l'unité. Prenons $OC = \frac{1}{4}$, puis, du point C comme centre, avec CA pour rayon, décrivons un cercle qui coupe en B et D la ligne UV ; on aura

$$OB = \frac{1}{2}y, \quad OD = \frac{1}{2}y';$$

car

$$2OD - 2OB = 4OC = 1 \quad \text{et} \quad 2OD \times 2OB = 4\overline{OA}^2 = 4.$$

2° Joignons AB, et du point B comme centre, avec OB pour rayon, décrivons une circonférence qui coupe en M

et P la ligne AB prolongée, on aura

$$AM = z, \quad AP = z';$$

car

$$AM - AP = PM = 2OB = y \quad \text{et} \quad AM \times AP = \overline{AO}^2 = 1.$$

Joignons pareillement AD, et du point D comme centre, avec OD pour rayon, décrivons une circonférence qui coupe en N et Q la ligne AD prolongée, on aura

$$AN = u, \quad AQ = u';$$

car

$$AQ - AN = NQ = 2OD = y' \quad \text{et} \quad AN \times AQ = \overline{AO}^2 = 1.$$

3° Rabattons AO en AE sur le prolongement de AD, décrivons sur NE, comme diamètre, un cercle qui coupe AB en F; du point F comme centre, avec $AI = \frac{AM}{2}$ pour rayon, décrivons un cercle qui coupe AD en G; et, enfin, du point G comme centre, avec ce même rayon, décrivons un cercle qui coupe AD en K et H, on aura

$$x_1 = AK, \quad x = AH;$$

car

$$AK + AH = 2GF = 2AI = AM = z$$

et

$$AK \times AH = \overline{AF}^2 = AN \times AE = AN \times AO = u.$$

Le côté du polygone régulier de trente-quatre côtés inscrit dans le cercle dont le rayon est OA est donc égal à AK.

Sur une propriété remarquable de la fonction $\frac{x^p - 1}{x - 1}$, p étant un nombre premier.

548. Soit p un nombre premier autre que 2, et posons

$$X = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1.$$

Désignons par a une racine primitive pour le nombre premier p, et par r une racine de l'équation

(1) $$X = 0;$$

les racines de l'équation (1) seront

$$r^a,\ r^{a^2},\ r^{a^3},\ \ldots,\ r^{a^{p-1}},$$

et l'on aura

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{et} \quad r^{a^{p-1}} = r.$$

Si l'on fait

$$y_1 = r^{a^2} + r^{a^4} + r^{a^6} + \ldots + r^{a^{p-1}},$$
$$y_2 = r^a + r^{a^3} + r^{a^5} + \ldots + r^{a^{p-2}},$$

les quantités y_1 et y_2 (n° 535) seront les racines d'une équation du deuxième degré à coefficients commensurables, et l'équation (1) se décomposera en deux autres, chacune du degré $\frac{p-1}{2}$, et dont les coefficients seront des fractions rationnelles de y_1 et de y_2. Nous nous proposons ici d'étudier les détails de la décomposition dont il s'agit.

Occupons-nous, en premier lieu, de former l'équation en y, qui a pour racines y_1 et y_2. On a d'abord

(2) $$y_1 + y_2 = -1,$$

car $y_1 + y_2$ exprime la somme de toutes les racines de l'équation (1). Ensuite, comme les fonctions symétriques de y_1 et de y_2 ne changent pas, quand on change r en r^a, ou en r^{a^2}, ou etc., on a

$$y_1^2 + y_2^2 = \frac{1}{\left(\frac{p-1}{2}\right)} \sum \left(x^{a^2} + x^{a^4} + x^{a^6} + \ldots + x^{a^{p-1}}\right)^2,$$

le signe $\sum$ s'étendant à toutes les racines x de l'équation (1).

Or on a

$$\left(x^{a^2}+x^{a^4}+\ldots+x^{a^{p-1}}\right)^2=\sum x^{a^{2m}+a^{2n}},$$

le signe $\sum$ s'étendant ici à toutes les valeurs 1, 2, 3,..., $\frac{p-1}{2}$ des entiers m et n; si donc on désigne par $S(\mu)$ la somme des puissances $\mu^{\text{ièmes}}$ des racines de l'équation (1), on aura

$$y_1^2+y_2^2=\frac{1}{\left(\frac{p-1}{2}\right)}\sum S\left(a^{2m}+a^{2n}\right);$$

le signe $\sum$ s'étend à toutes les valeurs 1, 2, 3 ,..., $\frac{p-1}{2}$ des entiers m et n, et il embrasse, en conséquence, $\left(\frac{p-1}{2}\right)^2$ termes. Comme a est une racine primitive de p, on a

$$a^{\frac{p-1}{2}}+1\equiv 0 \pmod{p},$$

et il ne saurait y avoir aucune puissance de a d'un degré inférieur à $\frac{p-1}{2}$ congrue à -1 suivant le module p. D'après cela, si p est de la forme $4i+1$, la somme

$$a^{2m}+a^{2n}$$

ne sera divisible par p que pour les $2i=\frac{p-1}{2}$ systèmes suivants de valeurs simultanées de m et n :

$$\begin{array}{llllllllll} m=1, & 2, & 3, & \ldots, & i, & i+1, & i+2, & \ldots, & 2i, \\ n=i+1, & i+2, & i+3, & \ldots, & 2i, & 1, & 2, & \ldots, & i; \end{array}$$

si p est de la forme $4i+3$, aucune des valeurs que prend la somme

$$a^{2m}+a^{2n}$$

n'est divisible par p.

La somme $S(\mu)$ est égale à $p-1$ ou à -1 (n° 106) suivant que μ est divisible ou non divisible par p; donc, si p a la forme $4i+1$, la quantité

$$\sum S(a^{2m}+a^{2n})$$

sera égale à

$$\frac{p-1}{2}(p-1)-\left[\left(\frac{p-1}{2}\right)^2-\left(\frac{p-1}{2}\right)\right];$$

si, au contraire, p a la forme $4i+3$, la même quantité sera égale à

$$-\left(\frac{p-1}{2}\right)^2.$$

On a ainsi

$$(3)\qquad y_1^2+y_2^2=\frac{1+p(-1)^{\frac{p-1}{2}}}{2}.$$

Des équations (2) et (3), on tire

$$(4)\qquad y_1y_2=\frac{1-p(-1)^{\frac{p-1}{2}}}{4}.$$

D'après cela, l'équation qui a pour racines y_1 et y_2 est

$$(5)\qquad y^2+y+\frac{1-p(-1)^{\frac{p-1}{2}}}{4}=0,$$

ou

$$(2y+1)^2-p(-1)^{\frac{p-1}{2}}=0.$$

519. Considérons maintenant l'équation qui a pour racines les $\frac{p-1}{2}$ racines de l'équation (1) dont y_1 dé-

signe la somme. Soit

$$X_1 = x^{\frac{p-1}{2}} - y_1 x^{\frac{p-1}{2}-1} + A_2 x^{\frac{p-1}{2}-2} + \ldots + A_k x^{\frac{p-1}{2}-k} + \ldots = 0$$

cette équation. Les coefficients A_2, A_3, ... peuvent s'exprimer par des fonctions rationnelles de y_1, et l'on peut supposer ces fonctions linéaires (n° 182), puisque y_1 est racine d'une équation du deuxième degré. Ainsi le coefficient A_k aura la forme

$$A_k = m_k + n_k y_1,$$

m_k et n_k étant des nombres rationnels, et il est facile de prouver que ces nombres sont entiers. En effet, A_k est, au signe près, la somme des produits k à k des $\frac{p-1}{2}$ racines r^{a^2}, r^{a^4}, ...; chacun de ces produits est une puissance de r, et, par suite, il se réduit à l'unité ou à l'une des racines de l'équation (1). On a donc

$$A_k = \alpha_0 + \alpha_1 r + \alpha_2 r^a + \alpha_3 r^{a^2} + \ldots + \alpha_{p-1} r^{a^{p-2}},$$

α_0, α_1, ... étant des nombres entiers. Cette valeur de A_k ne changera pas si l'on change r en r^{a^2} et, par suite, on aura

$$A_k = \alpha_0 + \alpha_1 r^{a^2} + \alpha_2 r^{a^3} + \alpha_3 r^{a^4} + \alpha_4 r^{a^5} + \ldots + \alpha_{p-1} r^{a}.$$

Je dis que les coefficients des mêmes puissances de r sont égaux dans ces deux valeurs de A_k. Supposons, en effet, que cela n'ait pas lieu; si l'on égale les deux valeurs de A_k et qu'on rabaisse les exposants de k au-dessous de p, en faisant usage de l'équation $r^p = 1$, on aura une équation du degré $p-1$ en r qui sera évidemment satisfaite par $r = 1$; on pourra enlever cette racine 1, et alors on voit que r sera une racine d'une équation du degré $p-2$

à coefficients commensurables, ce qui est impossible, puisque l'équation (1) est irréductible. On a donc

$$\alpha_1 = \alpha_3 = \alpha_5 = \ldots = \alpha_{p-2},$$
$$\alpha_2 = \alpha_4 = \alpha_6 = \ldots = \alpha_{p-1},$$

et, par suite,

$$A_k = \alpha_0 + \alpha_1 y_1 + \alpha_2 y_2.$$

Enfin, si l'on élimine y_2 à l'aide de l'équation (2), la valeur de A_k prendra la forme

$$A_k = m_k + n_k y_1,$$

où m_k et n_k désignent des nombres entiers positifs ou négatifs.

Le produit des racines de l'équation (6), savoir $r^{a^2+a^4+\ldots+a^{p-1}}$ est égal à 1, en exceptant le cas de $p=3$; car, a étant une racine primitive de p, l'exposant $a^2+a^4+\ldots+a^{p-1} = \dfrac{a^2(a^{p-1}-1)}{a^2-1}$ est divisible par p; on a donc

$$A_{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}}.$$

Comparons les coefficients A_k et $A_{k'}$ de deux termes également distants des extrêmes, dans X_1; on a la relation $k + k' = \dfrac{p-1}{2}$ entre les indices k et k'. La quantité $(-1)^k A_k$ est une somme de puissances de r, et la somme des inverses des mêmes puissances est égale à $(-1)^{k'} A_{k'}$; car le produit de toutes les racines de l'équation (6) est égal à 1. Cela posé, si $p = 4i + 1$, les suites

$$r^a,\ r^{a^3},\ \ldots,\ r^{a^{p-2}},$$
$$r^{a^2},\ r^{a^4},\ \ldots,\ r^{a^{p-1}}$$

restent les mêmes quand on change r en $\dfrac{1}{r}$; donc on a,

dans ce cas,

$$A_{k'} = A_k = m_k + n_k y_1.$$

Si $p = 4i + 3$, les suites

$$r^a,\ r^{a^3},\ldots,\ r^{a^{p-2}},$$
$$r^{a^2},\ r^{a^4},\ldots,\ r^{a^{p-1}}$$

se changent l'une en l'autre quand on change r en $\frac{1}{r}$; d'ailleurs k et k' sont de parités différentes ; donc l'équation

$$A_k = m_k + n_k y_1$$

entraîne

$$-A_{k'} = m_k + n_k y_2 = m_k - n_k(1 + y_1),$$

et l'on a, dans ce cas,

$$A_{k'} = (n_k - m_k) + n_k y_1.$$

Il résulte de là que le polynôme X_1 peut se mettre sous la forme suivante :

$$X_1 = P + Q y_1,$$

P et Q étant des polynômes à coefficients entiers qui ont respectivement pour degrés $\frac{p-1}{2}$ et $\frac{p-3}{2}$. En outre, Q est un polynôme divisible par x dans lequel les termes également distants des extrêmes sont égaux et de même signe; le polynôme P jouit de cette dernière propriété dans le cas de $p = 4i + 1$ seulement, et, par suite, il en est de même de la fonction $2P - Q$. Dans le cas de $p = 4i + 3$, la fonction $2P - Q$ a cette propriété, que les coefficients des termes également distants des extrêmes sont égaux et de signes contraires. En effet, les coefficients de $x^{\frac{p-1}{2}-k}$ et de x^k dans la fonction $2P - Q$ sont alors

$$2m_k - n_k \text{ et } n_k - 2m_k.$$

Pour obtenir les valeurs des coefficients A_2, A_3, ..., de X_1, soit λ l'un des nombres

$$1, 2, 3, \ldots, (p-1),$$

et h un exposant entier, tel que

$$a^h \equiv \lambda \pmod{p};$$

désignons enfin par S_λ la somme des puissances $\lambda^{\text{ièmes}}$ des racines de l'équation $X_1 = 0$, on aura

$$S_\lambda = r^{a^{h+2}} + r^{a^{h+4}} + \ldots + r^{a^{h+p-1}};$$

d'où il suit que S_λ sera égal à y_1 si h est pair, c'est-à-dire si λ est résidu quadratique de p. Au contraire, S_λ sera égal à y_2 ou à $-1-y_1$ si h est impair, c'est-à-dire si λ est non-résidu quadratique de p. Connaissant ainsi les sommes de puissances semblables des racines de l'équation (6), on calculera les coefficients A_2, A_3, ..., au moyen des formules

$$S_1 - y_1 = 0,$$
$$S_2 - y_1 S_1 + 2A_2 = 0,$$
$$S_3 - y_1 S_2 + 2A_2 S_1 + 3A_3 = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

On pourra exprimer ainsi A_k par une fonction entière de y_1 et l'on rendra ensuite cette fonction linéaire au moyen de l'équation (5).

550. L'analyse que nous venons de développer conduit à un théorème important que nous devons mentionner.

Reprenons l'équation

$$X_1 = P + Q y_1,$$

que nous avons trouvée plus haut ; en changeant y_1 en y_2,

on aura

$$X_2 = P + Q y_2;$$

on a d'ailleurs $X = X_1 X_2$, donc

$$X = P^2 + PQ(y_1 + y_2) + Q^2 y_1 y_2,$$

ou, à cause de

$$y_1 + y_2 = -1, \quad y_1 y_2 = \frac{1 - p(-1)^{\frac{p-1}{2}}}{4},$$

$$4X = (2P - Q)^2 - (-1)^{\frac{p-1}{2}} p Q^2.$$

Et, d'après les remarques faites précédemment, on peut énoncer ce théorème :

THÉORÈME. — *p étant un nombre premier autre que 2, et X désignant le polynôme*

$$x^{p-1} + x^{p-2} + \ldots + x + 1,$$

on aura

$$4X = Y^2 - pZ^2 \quad \text{si} \quad p = 4i + 1,$$

et

$$4X = Y^2 + pZ^2 \quad \text{si} \quad p = 4i + 3.$$

Z est, dans les deux cas, un polynôme du degré $\frac{p-3}{2}$ à coefficients entiers dans lequel les termes également distants des extrêmes ont le même coefficient; Y est un polynôme du degré $\frac{p-1}{2}$ à coefficients entiers dont les termes également distants des extrêmes ont des coefficients égaux et de même signe, ou égaux et de signes contraires, suivant que $p = 4i + 1$ ou $4i + 3$.

Le nombre 3 échappe à notre analyse, ainsi que nous en avons fait plus haut la remarque. L'équation

$$4(x^2 + x + 1) = Y^2 + 3Z^2$$

admet toutefois les trois solutions

$$Y = 2x + 1,\quad Z = 1,$$
$$Y = x + 2,\quad Z = x,$$
$$Y = x - 1;\quad Z = x + 1;$$

mais les polynômes Y et Z, relatifs à l'une quelconque de ces trois solutions, ne satisfont pas à toutes les conditions indiquées dans l'énoncé du théorème.

Enfin le résultat que nous venons de trouver relativement à la fonction $\frac{x^p - 1}{x - 1}$ peut s'étendre à la fonction plus générale $\frac{x^p - y^p}{x - y}$, qu'on déduit de la première en changeant x en $\frac{x}{y}$, et en multipliant ensuite par y^{p-1}. On peut évidemment, d'après cela, énoncer le théorème suivant :

Le nombre p étant premier, on peut satisfaire à l'équation

$$Y^2 - (-1)^{\frac{p-1}{2}} pZ^2 = 4\frac{x^p - y^p}{x - y},$$

en prenant pour Y *et* Z *des fonctions entières de* x *et* y.

Sur quelques propriétés de la fonction résolvante qui se rapporte à l'équation $\frac{x^p - 1}{x - 1} = 0$.

551. Soit, comme précédemment, x une quelconque des racines de l'équation $\frac{x^p - 1}{x - 1} = 0$, et a une racine primitive pour le nombre premier p. En désignant par x une racine quelconque de l'équation $\frac{x^{p-1} - 1}{x - 1} = 0$, nous po-

serons

$$F(\alpha) = x + \alpha x^a + \alpha^2 x^{a^2} + \ldots + \alpha^{p-2} x^{a^{p-2}} = \sum_{0}^{p-2}{}_i \alpha^i x^{a^i},$$

et nous allons en premier lieu démontrer que l'on a

$$F(\alpha) F(\alpha^{-1}) = \alpha^{\frac{p-1}{2}} p.$$

On a

$$F(\alpha^{-1}) = \sum_{0}^{p-2}{}_k \alpha^{-k} x^{a^k},$$

et, par conséquent,

$$F(\alpha) F(\alpha^{-1}) = \sum_{0}^{p-2}{}_k \sum_{0}^{p-2}{}_i \alpha^{i-k} x^{a^i + a^k}.$$

Pour évaluer cette somme double, je mettrai en évidence les coefficients des diverses puissances de α, et j'introduirai à cet effet le nombre entier

$$i - k = l.$$

Alors le coefficient de α^l sera

$$\sum x^{a^{k+l} + a^k},$$

le signe $\sum$ s'étendant aux $p - 1$ valeurs de k

$$0, 1, 2, \ldots, p - 2.$$

Or on peut écrire

$$a^{k+l} + a^k = a^k (a^l + 1);$$

si donc on n'a pas

$$a^l + 1 \equiv 0 \pmod{p},$$

c'est-à-dire

$$l = \frac{p-1}{2},$$

l'expression $a^k(a^l+1)$ donnera, pour les diverses valeurs de k et abstraction faite des multiples de p, la série des nombres

$$1,\ 2,\ \ldots,\ p-1.$$

Ainsi le coefficient de α^l sera

$$x + x^2 + \ldots + x^{p-1} \quad \text{ou bien} \quad -1,$$

et cette conclusion aura lieu pour toutes les valeurs

$$0,\ 1,\ 2,\ \ldots,\ p-2$$

de l, en exceptant le seul cas $l = \frac{p-1}{2}$. La somme double que nous avons à évaluer sera donc composée du produit de -1 par la somme des diverses puissances de α, sauf la puissance $\alpha^{\frac{p-1}{2}}$, et, en outre, du groupe de termes correspondant à la valeur $l = \frac{p-1}{2}$. Lorsque $l = \frac{p-1}{2}$, l'exposant de x est congru à zéro pour toutes les valeurs de k; par conséquent, le groupe que nous considérons sera composé de $(p-1)$ fois la racine $\alpha^{\frac{p-1}{2}}$. Réunissant ces deux parties de la somme double, on trouve pour résultat

$$\alpha^{\frac{p-1}{2}}(p-1) + \alpha^{\frac{p-1}{2}} = \alpha^{\frac{p-1}{2}} p,$$

ce qui démontre le théorème énoncé.

552. Nous allons maintenant établir une seconde proposition qui consiste en ce que, si m et n sont deux nombres entiers quelconques, mais non liés par la relation

$$m \equiv -n \pmod{p},$$

le produit $F(\alpha^m)F(\alpha^n)$ est égal à la fonction $F(\alpha^{m+n})$, multipliée par un polynôme en α, dont les coefficients sont des nombres entiers. Ainsi, en désignant par $\psi(\alpha)$ ce polynôme, on aura l'égalité

$$F(\alpha^m\ F(\alpha^n) = F(\alpha^{m+n})\,\psi(\alpha).$$

En effet, on a

$$F(\alpha^m) = \sum \alpha^{mi} x^{a^i},$$

$$F(\alpha^n) = \sum \alpha^{nk} x^{a^k},$$

donc

$$F(\alpha^m)\,F(\alpha^n) = \sum\sum \alpha^{mi+nk} x^{a^i+a^k},$$

et c'est la somme double du second membre qu'il s'agit d'évaluer sous la forme annoncée. Pour cela nous allons mettre en évidence, non plus les coefficients des diverses puissances de α, comme précédemment, mais les coefficients des puissances de x. Ces puissances formant la série $0, 1, 2, \ldots, p-1$, occupons-nous d'abord du premier terme qui proviendra de toutes les valeurs de i et k, telles qu'on ait

$$a^i + a^k \equiv 0 \pmod{p},$$

c'est-à-dire

$$i - k = \frac{p-1}{2}.$$

Sous cette condition, la somme

$$\sum \alpha^{mi+nk} = \sum \alpha^{m\left(k+\frac{p-1}{2}\right)+nk} = \alpha^{\frac{m(p-1)}{2}} \sum \alpha^{(m+n)k}$$

s'évanouit, car n'ayant pas $m+n \equiv 0 \pmod{p}$, l'expression $(m+n)k$ produit la série des entiers inférieurs à p, comme on le sait.

Maintenant, pour mettre en évidence le coefficient

d'une puissance quelconque de x, dont l'exposant serait $\equiv a^l$, posons

$$a^i + a^k \equiv a^l \pmod{p};$$

ce coefficient sera

$$\sum \alpha^{mi+nk},$$

les entiers i et k devant prendre toutes les valeurs qui peuvent vérifier la précédente condition. Si l'on fait

$$\begin{aligned} i &= l + \mu, \\ k &= l + \nu, \end{aligned}$$

la condition dont il s'agit devient indépendante de l, et elle se réduit à

$$a^\mu + a^\nu \equiv 1 \pmod{p}.$$

Nous pouvons concevoir que, pour une valeur donnée du nombre premier p, on ait formé d'avance le système des nombres μ et ν, liés par cette relation ; cela fait, on trouvera

$$\sum \alpha^{mi+nk} = \sum \alpha^{m(l+\mu)+n(l+\nu)} = \alpha^{(m+n)l} \sum \alpha^{m\mu+n\nu}.$$

Donc, si l'on pose

$$\psi(\alpha) = \sum \alpha^{m\mu+n\nu},$$

le coefficient de x^{a^l} sera

$$\alpha^{(m+n)l}\,\psi(\alpha),$$

et la somme double sera bien, comme nous l'avons annoncé,

$$\psi(\alpha) \sum \alpha^{(m+n)l}\, x^{a^l} = \psi(\alpha)\, F(\alpha^{m+n}).$$

553. Ces polynômes, ou plutôt ces nombres *complexes*,

$\psi(\alpha)$, dont la formation dépend essentiellement des entiers μ et ν, et ensuite des nombres m et n, conduisent à d'admirables théorèmes arithmétiques dont nous allons donner quelques exemples.

J'observe d'abord que la relation

$$F(\alpha^m)F(\alpha^n) = F(\alpha^{m+n})\psi(\alpha)$$

donnera, en changeant les signes de m et n,

$$F(\alpha^{-m})F(\alpha^{-n}) = F[\alpha^{-(m+n)}]\psi(\alpha^{-1}).$$

Multipliant membre à membre, et ayant égard à la relation

$$F(\alpha)F(\alpha^{-1}) = \alpha^{\frac{p-1}{2}}p,$$

on trouve immédiatement

$$\psi(\alpha)\psi(\alpha^{-1}) = p.$$

Un cas particulier très-simple montrera tout l'intérêt qui s'attache à ce résultat. Soit

$$p \equiv 1 \pmod{4},$$

on satisfera à l'équation

$$\alpha^{p-1} = 1,$$

en prenant

$$\alpha = \sqrt{-1} = i.$$

Alors $\psi(\alpha)$, somme de puissances entières de i, sera de la forme $a + bi$, a et b étant entiers ; d'ailleurs $\frac{1}{\alpha} = \frac{1}{i}$ aura pour valeur $-i$, de sorte que

$$\psi(\alpha^{-1}) = a - bi;$$

donc tout nombre premier $\equiv 1 \pmod{4}$ est de la forme

$$(a + bi)(a - bi) = a^2 + b^2.$$

Ce théorème, qui a été établi par une méthode si diffé-

Donc on a, dans tous les cas,

$$Q = \left(\frac{q}{p}\right) P,$$

et, par suite,

$$P^q = \left(\frac{q}{p}\right) P + q \sum A r^\alpha,$$

ou

$$(1) \qquad P^{q-1} - \left(\frac{q}{p}\right) = q \frac{\sum A r^\alpha}{P}.$$

Cela posé, si l'on fait

$$y_1 = r \;\; + r^{a^2} + r^{a^4} + \ldots + r^{a^{p-3}},$$
$$y_2 = r^a + r^{a^3} + r^{a^5} + \ldots + r^{a^{p-2}},$$

on aura (n° 548)

$$y_1 = -\frac{1}{2} \pm \frac{1}{2} \sqrt{(-1)^{\frac{p-1}{2}} p},$$

$$y_2 = -\frac{1}{2} \mp \frac{1}{2} \sqrt{(-1)^{\frac{p-1}{2}} p};$$

d'où

$$P = y_1 - y_2 = \pm \sqrt{(-1)^{\frac{p-1}{2}} p}.$$

Substituant cette valeur de P dans le premier membre de la formule (1), celui-ci se réduit à

$$p^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2} \frac{q-1}{2}} - \left(\frac{q}{p}\right),$$

quantité qui est un nombre entier. Quant au second membre $q \frac{\sum A r^\alpha}{P}$, il se réduira donc aussi à un nombre

entier E, et l'on aura

$$\left(\sum \mathrm{A} r^{\alpha}\right)^{2} = (-1)^{\frac{p-1}{2}} \frac{p \mathrm{E}^{2}}{q^{2}}.$$

Il s'ensuit que le carré de $\sum \mathrm{A} r^{\alpha}$ est une fonction symétrique et entière des racines de l'équation $\frac{x^p - 1}{x - 1} = 0$; par suite, ce carré a pour valeur un nombre entier, ce qui exige que E soit un multiple Mq de q. Ainsi l'on a

$$q \frac{\sum \mathrm{A} r^{\alpha}}{\mathrm{P}} = \mathrm{E} = \mathrm{M} q,$$

M étant un nombre entier. Par conséquent,

$$p^{\frac{q-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} - \left(\frac{q}{p}\right) = \mathrm{M} q;$$

remarquant que

$$p^{\frac{q-1}{2}} = \left(\frac{p}{q}\right) + \text{un multiple de } q,$$

et supprimant de part et d'autre les multiples de q, il vient

$$(2) \qquad \left(\frac{p}{q}\right) (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{q}{p}\right);$$

cette formule (2) exprime précisément le théorème de Legendre.

CHAPITRE IV.

SUR UNE CLASSE D'ÉQUATIONS DU NEUVIÈME DEGRÉ RÉSOLUBLES ALGÉBRIQUEMENT.

Du déterminant d'une fonction entière et homogène de trois variables.

556. Otto Hesse a publié dans le *Journal de Crelle* (t. XXVIII, p. 68, et t. XXXIV, p. 191) deux Mémoires remarquables sur la détermination des points d'inflexion des courbes du troisième degré. Dans son second Mémoire, l'éminent géomètre a démontré que :

Les points d'inflexion d'une courbe algébrique du degré n sont situés sur une seconde courbe du degré $3(n-2)$, et, par suite, que :

Une courbe algébrique du degré n a généralement $3n(n-2)$ *points d'inflexion, réels ou imaginaires.*

Dans les cas particuliers, quelques-uns de ces points d'inflexion peuvent être situés à l'infini ou être remplacés par des points multiples.

Lorsque $n=3$, on a ce théorème :

Les points d'inflexion d'une courbe du troisième degré sont situés sur une seconde courbe du troisième degré.

Il en résulte que la recherche des points d'inflexion d'une courbe du troisième degré dépend généralement de la résolution d'une équation du neuvième degré à une inconnue. Or il est très-remarquable que cette équation

du neuvième degré soit toujours résoluble algébriquement, et qu'il suffise, pour effectuer cette résolution, de résoudre une seule équation du quatrième degré et trois équations du troisième dégré. Cette proposition se déduit facilement, comme nous le ferons voir plus loin, du théorème de Hesse énoncé plus haut, et d'un autre théorème démontré pour la première fois par Maclaurin dans son *Essai sur les lignes du troisième degré*, théorème qui consiste en ce que :

La droite qui joint deux points d'inflexion d'une courbe du troisième degré rencontre la courbe en un troisième point d'inflexion.

La démonstration que Hesse a donnée dans son second Mémoire, pour établir la résolubilité de l'équation du neuvième degré dont il s'agit, suppose également le théorème de Maclaurin. Hesse fait voir qu'il existe certaines relations entre les racines, et il démontre généralement que toute équation du neuvième degré dont les racines ont cette même propriété est résoluble par radicaux. Cette analyse de Hesse est remarquable; on en trouvera le développement à la fin de ce Chapitre.

557. Soit U une fonction quelconque entière et homogène du $n^{\text{ième}}$ degré de deux variables x et y; $U = 0$ sera une équation quelconque du degré n si l'on prend pour inconnue $\frac{x}{y}$, et cette équation aura trois racines égales si l'on peut satisfaire en même temps aux trois équations

$$U = 0, \quad \frac{dU}{dx} = 0, \quad \frac{d^2U}{dx^2} = 0.$$

Ces équations de condition sont respectivement des degrés n, $n-1$, $n-2$; mais on peut à leur place prendre trois équations du même degré $n-2$. Elles peuvent ef-

fectivement s'écrire ainsi (*) :

$$U = \frac{1}{n(n-1)}\left(x^2\frac{d^2U}{dx^2} + 2xy\frac{d^2U}{dx\,dy} + y^2\frac{d^2U}{dy^2}\right) = 0,$$

$$\frac{dU}{dx} = \frac{1}{n-1}\left(x\frac{d^2U}{dx^2} + y\frac{d^2U}{dx\,dy}\right) = 0,$$

$$\frac{d^2U}{dx^2} = 0.$$

A cause de la troisième équation, la deuxième se réduit à $\frac{d^2U}{dx\,dy} = 0$, et la première devient ensuite $\frac{d^2U}{dy^2} = 0$. Donc les équations de condition relatives à l'égalité de trois racines de l'équation $U = 0$ sont les suivantes du degré $n-2$ chacune :

$$\frac{d^2U}{dx^2} = 0,\quad \frac{d^2U}{dx\,dy} = 0,\quad \frac{d^2U}{dy^2} = 0.$$

On ferait voir de même que généralement les équations de condition relatives à l'égalité de m racines de l'équation $U = 0$ sont les suivantes, du degré $n-m+1$:

$$\frac{d^{m-1}U}{dx^{m-1}} = 0,\quad \frac{d^{m-1}U}{dx^{m-2}\,dy} = 0,\quad \ldots,\quad \frac{d^{m-1}U}{dx\,dy^{m-2}} = 0,\quad \frac{d^{m-1}U}{dy^{m-1}} = 0.$$

(*) Cela résulte immédiatement du théorème connu dit *des fonctions homogènes*. Soit $f(x, y, \ldots)$ une fonction homogène du degré μ de plusieurs variables; en multipliant $x, y, \ldots$ par $1+\alpha$, il vient, d'après la définition des fonctions homogènes,

$$f(x+\alpha x, y+\alpha y, \ldots) = (1+\alpha)^\mu f(x, y, \ldots).$$

Développant les deux membres par rapport à α et égalant ensuite les coefficients des mêmes puissances de α, il vient

$$x\frac{df}{dx} + y\frac{df}{dy} + \ldots = \mu f(x, y, \ldots),$$

$$x^2\frac{d^2f}{dx^2} + 2xy\frac{d^2f}{dx\,dy} + y^2\frac{d^2f}{dy^2} + \ldots = \mu(\mu-1)f(x, y, \ldots),$$

....

558. Soit maintenant u une fonction quelconque entière et homogène, du $n^{\text{ième}}$ degré, de trois variables x, y, z. Si l'on représente par $\frac{x}{z}$ et $\frac{y}{z}$ les coordonnées rectangulaires ou obliques d'un point variable, l'équation

$$(1)\qquad u = 0$$

représentera une courbe quelconque du $n^{\text{ième}}$ degré ([1]).

Une droite quelconque, dont l'équation est

$$(2)\qquad z = ax + by,$$

rencontre, comme on sait, la courbe en n points; si l'on porte la valeur de z tirée de l'équation (2) dans la fonction u, celle-ci devient une fonction homogène U des deux variables x et y, et les n racines de l'équation $\mathrm{U} = 0$, où l'on considère $\frac{x}{y}$ comme l'inconnue, sont les rapports des coordonnées des points où la droite rencontre la courbe. Mais l'équation de la ligne droite contient deux constantes a et b qui s'introduisent dans l'équation $\mathrm{U} = 0$; on peut établir entre ces constantes une relation telle, que deux racines de l'équation $\mathrm{U} = 0$ deviennent égales : dans ce cas, la droite devient une tangente de la courbe. Et, si l'on donne aux constantes a et b des valeurs telles, que trois racines de l'équation $\mathrm{U} = 0$ deviennent égales, la droite sera tangente en un point d'inflexion ; ce point sera déterminé, commme on

---

([1]) Hesse a eu le premier l'ingénieuse idée de représenter par $\frac{x}{z}$, $\frac{y}{z}$ les coordonnées rectilignes d'un point dans un plan, et par $\frac{x}{u}$, $\frac{y}{u}$, $\frac{z}{u}$ les coordonnées dans l'espace; alors toutes les équations que l'on a à considérer sont homogènes.

l'a vu plus haut, par les trois équations

$$\frac{d^2U}{dx^2} = 0, \quad \frac{d^2U}{dx\,dy} = 0, \quad \frac{d^2U}{dy^2} = 0.$$

Mais, comme U est la valeur que prend u pour $z = ax + by$, si l'on fait, pour abréger,

$$\frac{d^2u}{dx^2} = u_{1,1}, \quad \frac{d^2u}{dy^2} = u_{2,2}, \quad \frac{d^2u}{dz^2} = u_{3,3},$$

$$\frac{d^2u}{dy\,dz} = u_{2,3}, \quad \frac{d^2u}{dx\,dz} = u_{3,1}, \quad \frac{d^2u}{dx\,dy} = u_{1,2},$$

les trois équations précédentes pourront s'écrire comme il suit :

$$(3)\quad \left\{\begin{aligned} u_{1,1} + 2au_{3,1} + a^2u_{3,3} &= 0,\\ u_{1,2} + au_{2,3} + bu_{3,1} + abu_{3,3} &= 0,\\ u_{2,2} + 2bu_{2,3} + b^2u_{3,3} &= 0. \end{aligned}\right.$$

Si l'on élimine a et b entre ces équations, on obtiendra l'équation d'une courbe qui rencontre la proposée aux points d'inflexion. Pour effectuer cette élimination, résolvons la deuxième des équations (3) par rapport à a, ce qui donne

$$a = -\frac{u_{1,2} + bu_{3,1}}{u_{2,3} + bu_{3,3}},$$

et portons cette valeur dans la première équation, nous obtenons

$$u_{1,1}(u_{2,3} + bu_{3,3})^2 - 2u_{3,1}(u_{1,2} + bu_{3,1})(u_{2,3} + bu_{3,3}) + u_{3,3}(u_{1,2} + bu_{3,1})^2 = 0$$

ou, en ordonnant par rapport à b,

$$u_{1,1}u_{2,3}^2 - 2u_{2,3}u_{3,1}u_{1,2} + u_{3,3}u_{1,2}^2 + (u_{1,1}u_{3,3} - u_{3,1}^2)(2bu_{2,3} + b^2u_{3,3}) = 0.$$

Si enfin on multiplie la dernière des trois équations que nous considérons par

$$u_{1,1}u_{3,3} - u_{3,1}^2,$$

et qu'on en retranche ensuite l'équation que nous venons de former, on obtiendra l'équation finale qui résulte de l'élimination de a et b; nous la représenterons par

$$(4) \qquad \Delta u = 0,$$

en posant, pour abréger,

$$\Delta u = u_{1,1}\, u_{2,2}\, u_{3,3} + 2\, u_{2,3}\, u_{3,1}\, u_{1,2} - u_{1,1}\, u_{2,3}^2 - u_{2,2}\, u_{3,1}^2 - u_{3,3}\, u_{1,2}^2.$$

L'équation (4) est celle de la courbe cherchée, laquelle rencontre la proposée $u = 0$ aux points d'inflexion. Cette équation est, comme on voit, du degré $3(n-2)$, d'où il suit qu'une courbe du $n^{\text{ième}}$ degré a généralement $3n(n-2)$ points d'inflexion. En particulier, une courbe du troisième degré a neuf points d'inflexion.

La fonction Δu est égale au déterminant

$$\begin{vmatrix} u_{1,1} & u_{1,2} & u_{1,3} \\ u_{2,1} & u_{2,2} & u_{2,3} \\ u_{3,1} & u_{3,2} & u_{3,3} \end{vmatrix},$$

et Hesse lui a donné le nom de *déterminant de la fonction u*.

559. Lorsque les coefficients de la fonction u sont indéterminés, la courbe représentée par l'équation $u = 0$ n'a pas de points multiples. Pour de tels points on a simultanément

$$\frac{du}{dx} = 0, \quad \frac{du}{dy} = 0, \quad u = 0,$$

et, au moyen des deux premières équations, la troisième se réduit à

$$\frac{du}{dz} = 0,$$

par le théorème des fonctions homogènes. La relation entre les coefficients de u, exigée par l'existence de

points multiples, résultera donc de l'élimination de x et y entre

$$\frac{du}{dx}=0,\quad \frac{du}{dy}=0,\quad \frac{du}{dz}=0.$$

Ces équations peuvent être mises sous la forme

$$xu_{1,1}+yu_{1,2}+zu_{1,3}=0,$$
$$xu_{2,1}+yu_{2,2}+zu_{2,3}=0,$$
$$xu_{3,1}+yu_{3,2}+zu_{3,3}=0,$$

et l'on en déduit évidemment

$$\Delta u=0.$$

Au reste, la méthode dont nous avons fait usage pour trouver les points d'inflexion montre que les points multiples, quand il en existe, satisfont à la précédente équation; car, si la droite $z=ax+by$ devient tangente à la courbe en un point multiple, l'équation qui résulte de l'élimination de z entre

$$u=0 \quad \text{et} \quad z=ax+by$$

aura évidemment trois racines égales.

Il est facile de voir qu'une courbe du troisième degré ne peut avoir un point triple ou trois points doubles à moins qu'elle ne se réduise à un système de trois droites; elle ne peut non plus avoir deux points doubles à moins qu'elle ne se réduise au système formé d'une conique et d'une droite.

560. Le calcul que nous avons fait au n° 558 ne diffère pas de celui qu'il faudrait exécuter si l'on voulait obtenir la condition pour que la droite (2) fît partie du lieu représenté par l'équation (1). En effet, la solution de ce nouveau problème s'obtiendra en exprimant que le résultat U de la substitution de $ax+by$ à z, dans u,

est identiquement nul. On aura donc

$$\frac{d^2U}{dx^2}=0,\quad \frac{d^2U}{dx\,dy}=0,\quad \frac{d^2U}{dy^2}=0,$$

et il est évident que ces conditions sont suffisantes, puisque l'on a

$$n(n-1)U=x^2\frac{d^2U}{dx^2}+2xy\frac{d^2U}{dx\,dy}+y^2\frac{d^2U}{dy^2}.$$

Ainsi, dans le cas qui nous occupe, les équations (3) ont lieu identiquement en vertu de l'équation (2), et par conséquent il en est de même de l'équation (4). Donc toute droite qui fait partie du lieu de l'équation $u=0$ appartient aussi au lieu de l'équation $\Delta u=0$.

Dans le cas de $n=3$, on a ce théorème :

Si l'équation $u=0$ représente trois lignes droites, ces mêmes droites constituent le lieu de l'équation $\Delta u=0$, et l'on a en conséquence $\Delta u=ku$, k étant une constante.

Il peut arriver que le déterminant Δu soit identiquement nul; pour qu'il en soit ainsi, il faut et il suffit que le lieu de l'équation $u=0$ soit un faisceau de n lignes droites. Bien que nous n'eussions pas à faire usage de ce théorème dû à Hesse, nous ne pouvions nous dispenser de le mentionner ici.

Sur les points d'inflexion des courbes du troisième degré.

561. Nous commencerons par établir, à l'égard des courbes du troisième degré, quelques propositions générales sur lesquelles nous aurons à nous appuyer.

Rappelons d'abord que le système formé d'une conique et d'une droite, ou le système de trois droites, constitue une variété des lignes du troisième degré.

LEMME I. — *Deux courbes du troisième degré se coupent généralement en neuf points.*

Cette proposition se déduit immédiatement du théorème de Bézout sur le degré de l'équation finale qui résulte de l'élimination d'une inconnue entre deux équations.

562. LEMME II. — *Neuf points suffisent, en général, pour déterminer une courbe du troisième degré.*

Il y a effectivement dix termes dans l'équation générale des courbes du troisième degré. Le coefficient de l'un de ces termes peut être choisi arbitrairement, et il reste alors neuf coefficients indéterminés dont on peut disposer de manière à assujettir la courbe à passer par neuf points donnés. On obtient ainsi neuf équations du premier degré entre les coefficients inconnus; en général, ces équations admettent une solution unique, et, par suite, on ne peut généralement faire passer qu'une seule courbe du troisième degré par neuf points donnés (¹).

COROLLAIRE. — *Si $u = 0$, $v = 0$ sont les équations en coordonnées rectilignes de deux courbes du troisième degré, l'équation générale des courbes du troisième degré qui passent par les points communs aux courbes données sera*

$$v + \lambda u = 0,$$

λ désignant une constante indéterminée.

D'abord il est évident que l'équation $v + \lambda u = 0$ re-

---

(¹) Dans ses belles recherches sur les courbes du troisième et du quatrième degré (*voir* les *Comptes rendus de l'Académie des Sciences*, t. XXVI, p. 943, et t. XXVII, p. 272, 437 et 472), M. Chasles a fait connaître deux méthodes remarquables pour construire la courbe du troisième degré qui passe par neuf points donnés.

présente une courbe qui passe par les points d'intersection des courbes données. En second lieu, soit C l'une quelconque des courbes du troisième degré qui passent par ces neuf points ; prenons sur cette courbe un point quelconque M qui n'appartienne pas aux courbes données et désignons par v_1, u_1 ce que deviennent v et u, pour le point M. Si l'on détermine λ par la condition $v_1 + \lambda u_1 = 0$, la courbe représentée par l'équation $v + \lambda z = 0$ passera par le point M; cette courbe ayant ainsi dix points communs avec la courbe C, elle coïncide avec elle.

La démonstration précédente ne s'applique pas au cas où les lieux des équations $u = 0$, $v = 0$ auraient une droite commune ou une conique commune. Mais, dans ce cas, on a

$$v = tv', \quad u = tu';$$

$v' = 0$, $u' = 0$ représentent des droites ou des coniques, et $v' + \lambda u' = 0$ représente toute droite et toute conique qui passe par leurs points d'intersection. Il s'ensuit que $v + \lambda u = 0$ représente encore toutes les courbes du troisième degré qui passent par les points communs aux proposées.

563. Lemme III. — *Soient* A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8, A_9 *les neuf points d'intersection de deux courbes du troisième degré données; on peut faire passer par sept quelconques de ces points une infinité de lignes du troisième ordre qui ne passent par aucun des deux autres points.*

Considérons les sept points

$$A_1, A_2, A_3, A_4, A_5, A_6, A_7$$

Si trois d'entre eux, A_1, A_2, A_3, par exemple, sont en ligne droite, il existera trois systèmes formés de deux

droites tels, que chaque système renferme les quatre points A_4, A_5, A_6, A_7. L'une de ces six droites peut passer par A_8 ou par A_9, mais elle ne saurait contenir en même temps ces deux points, car une courbe du troisième degré ne peut avoir plus de trois points en ligne droite; donc, parmi nos trois systèmes de droites, il y en a au moins un qui ne renferme aucun des points A_8, A_9. Ce système constituera, avec la droite $A_1 A_2 A_3$, une ligne du troisième ordre qui remplira la condition énoncée.

Si, parmi les six points considérés, il y en a six qui soient sur une conique, cette conique n'aura aucun autre point commun avec l'une ou l'autre des courbes données, et par suite elle ne passera ni par A_8 ni par A_9. Si donc on joint à cette conique une droite arbitraire menée par le septième des points considérés et qui ne passe ni par A_8 ni par A_9, on aura une ligne du troisième ordre qui remplira encore la condition énoncée.

Supposons maintenant que parmi les sept points considérés il n'y en ait pas six sur une conique ni trois en ligne droite. Joignons le point A_7 aux six autres; parmi les six droites obtenues,

$$A_1 A_7,\quad A_2 A_7,\quad A_3 A_7,\quad A_4 A_7,\quad A_5 A_7,\quad A_6 A_7,$$

il ne saurait y en avoir plus d'une passant par A_8, ni plus d'une passant par A_9; on peut donc supposer que

$$A_3 A_7,\quad A_4 A_7,\quad A_5 A_7,\quad A_6 A_7$$

ne passent ni par A_8 ni par A_9. Pareillement, si l'on joint le plan A_6 aux points A_3, A_4, A_5, on obtiendra les trois droites

$$A_3 A_6,\quad A_4 A_6,\quad A_5 A_6,$$

parmi lesquelles il s'en trouvera une au moins qui ne passera ni par A_8 ni par A_9. D'où il suit que, parmi les

sept points considérés, on peut toujours en trouver trois

$$A_5, A_6, A_7,$$

par exemple, tels que les droites qui joignent ces points deux à deux ne passent par aucun des points A_8, A_9.

Cela posé, considérons les lignes du troisième ordre formées respectivement des coniques qui passent par A_1, A_2, A_3, A_4, A_5; A_1, A_2, A_3, A_4, A_6; A_1, A_2, A_3, A_4, A_7 et des droites

$$A_6A_7, A_5A_7, A_5A_6.$$

L'une des coniques peut contenir l'un des points A_8, A_9, mais non pas ces deux points à la fois, car une conique ne peut rencontrer une ligne du troisième ordre en plus de six points. D'ailleurs deux de nos coniques ne peuvent avoir que les seuls points communs A_1, A_2, A_3, A_4; donc l'une d'elles au moins, $A_1A_2A_3A_4A_5$, par exemple, ne contient ni A_8 ni A_9. En joignant à cette conique la droite A_6A_7, on formera une ligne du troisième ordre remplissant la condition énoncée.

Ainsi, dans tous les cas, nous savons trouver une ligne du troisième ordre qui passe par les sept points considérés et qui ne contient aucun des deux autres points. Soit

$$w = 0$$

l'équation de cette ligne relativement à deux axes coordonnés. Soient aussi

$$u = 0, \quad v = 0$$

les équations des courbes données, a et b deux constantes arbitraires; il est évident que l'équation

$$au + bv + w = 0$$

représentera une infinité de courbes du troisième degré, qui toutes rempliront la condition énoncée.

564. THÉORÈME I. — *Toute courbe du troisième degré, qui passe par huit des neuf points d'intersection de deux courbes du troisième degré données, passe également par le neuvième point d'intersection de ces deux courbes.*

Soient Γ et Γ_1 les deux courbes du troisième degré données. Supposons qu'on se propose de faire passer une courbe du troisième degré par les neuf points d'intersection des courbes Γ et Γ_1 ; les neuf équations linéaires que doivent vérifier les coefficients de l'équation de la courbe inconnue admettront les deux solutions relatives aux courbes Γ et Γ_1 qui satisfont au problème. Il s'ensuit que le système de ces neuf équations est indéterminé ; d'ailleurs huit quelconques d'entre elles sont distinctes, d'après le lemme III, et en conséquence elles entraînent nécessairement la neuvième. On peut conclure de là que, si l'on assujettit une courbe du troisième degré Γ_2 à passer par huit des points communs aux courbes Γ et Γ_1, et que, pour achever de la déterminer, on se donne une nouvelle condition arbitraire, la courbe Γ_2 passera nécessairement par le neuvième point d'intersection des courbes Γ et Γ_1.

COROLLAIRE I. — *Si trois des neuf points d'intersection des deux courbes du troisième degré sont en ligne droite, les six autres points d'intersection sont situés sur une conique.*

En effet, la droite qui passe par les trois premiers points d'intersection des courbes données Γ et Γ_1, et la conique qui passe par cinq des six autres, forment une ligne du troisième degré qui passe par le neuvième point d'intersection des courbes Γ et Γ_1 ; donc la conique passe par ce neuvième point, car une courbe du troisième degré ne peut avoir quatre points en ligne droite.

Corollaire II. — *Si six des neuf points d'intersection de deux courbes du troisième degré sont situés sur une conique, les trois autres points d'intersection sont en ligne droite.*

En effet, la conique qui passe par les six premiers points d'intersection et la droite qui passe par deux des trois autres forment une ligne du troisième degré qui passe par le neuvième point d'intersection ; donc la droite passe par ce neuvième point, car une conique ne peut avoir plus de six points communs avec une courbe du troisième degré.

Corollaire III. — *Si trois des neuf points d'intersection de deux courbes du troisième degré sont en ligne droite, et que trois des six autres soient aussi en ligne droite, les trois derniers seront pareillement en ligne droite.*

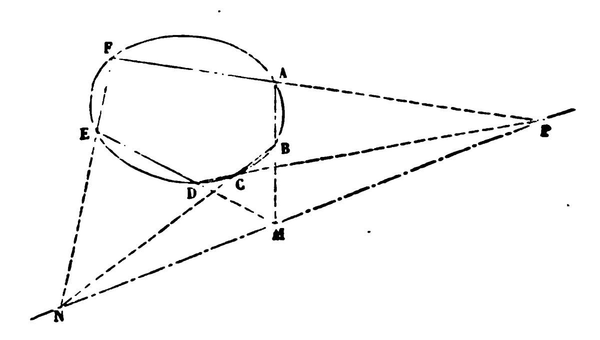
Ce corollaire est évidemment un cas particulier du précédent.

565. Les propositions que nous venons d'établir conduisent à un grand nombre de conséquences intéressantes ; mais, pour ne pas trop nous écarter de notre sujet, nous nous bornerons à montrer comment on en déduit immédiatement le théorème connu de Pascal, relatif à l'hexagone inscrit dans une conique. On sait que ce théorème consiste en ce que :

Si un hexagone est inscrit dans une conique, les points de rencontre des côtés opposés sont en ligne droite.

En effet, soient A, B, C, D, E, F les sommets de l'hexagone ; soient M, N, P les points d'intersection des côtés AB et DE, BC et EF, CD et FA. Les lignes du troisième ordre formées, l'une des droites AB, CD, EF, l'autre des

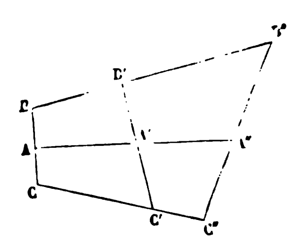
droites BC, DE, FA, se coupent aux neuf points A, B, C, D, E, F, M, N, P. Or les six premiers points sont une



conique; donc les trois autres sont en ligne droite, ce qu'il fallait démontrer.

566. Théorème II. — *La droite qui joint deux points d'inflexion d'une courbe du troisième degré rencontre la courbe en un troisième point d'inflexion.*

Soient A et A′ deux points d'inflexion d'une courbe du troisième degré Γ, et supposons que la droite AA′ rencontre la courbe Γ au troisième point A″; je dis que A″



est un point d'inflexion. En effet, menons par le point A une sécante quelconque qui rencontre de nouveau la courbe aux points B et C; par le point A une seconde sécante quelconque qui rencontre de nouveau la courbe

aux points B' et C'; joignons BB' et CC', qui rencontrent de nouveau la courbe aux points B'' et C'' respectivement; joignons enfin $A''B''$. La ligne du troisième degré formée des trois droites ABC, $A'B'C'$ et $A''B''$ passe par huit des points d'intersection de la courbe Γ et de la ligne du troisième degré formée de droites $AA'A''$, $BB'B''$, $CC'C''$: elle passera donc par le neuvième point d'intersection C''; et, comme une courbe de troisième degré ne peut avoir quatre points en ligne droite, il faut nécessairement que les trois points A'', B'', C'' soient en ligne droite. Imaginons maintenant que les sécantes BC et $B'C'$ tournent respectivement autour des points A et A', de manière à devenir tangentes à la courbe; comme A et A' sont deux points d'inflexion, les points B et C se confondront avec A à la limite : pareillement, B' et C' se confondront avec A'; donc les droites $BB'B''$ et $CC'C''$ coïncideront avec $AA'A''$, et, par suite, les trois points d'intersection de la courbe avec la sécante $A''B''C''$ se confondront en un seul A'', qui est ainsi un point d'inflexion.

Remarque. — Bien que la forme de ce raisonnement soit géométrique, il est évident qu'il s'applique au cas des points imaginaires comme à celui des points réels.

567. Théorème III. — *Le nombre des droites qui passent chacune par trois points d'inflexion d'une courbe du troisième degré donnée est égal à douze. Ces douze droites forment quatre systèmes composés chacun de trois droites, et les neuf points d'inflexion de la courbe sont trois à trois sur les trois droites de chaque système.*

Si l'on joint par des droites l'un des points d'inflexion de la courbe à chacun des huit autres, il est évident que ces huit droites se réduiront à quatre distinctes, puisque la droite qui passe par deux points d'inflexion passe

aussi par un troisième, et que, d'ailleurs, quatre points d'inflexion ne sauraient être en ligne droite. Donc, parmi les droites qui joignent les neuf points d'inflexion trois à trois, il y en a toujours quatre qui passent par l'un quelconque de ces points. En comptant quatre droites pour chaque point d'inflexion, on aura 4×9 ou trente-six droites; mais alors il est clair que chaque droite se trouve prise trois fois, et, par suite, ces trente-six droites se réduisent à douze distinctes.

Considérons l'une des quatre droites qui passent par un même point d'inflexion; cette droite renferme trois points d'inflexion, et par chacun de ceux-ci passent seulement trois autres de nos douze droites; donc, parmi ces douze droites, il y en a deux qui ne passent par aucun des trois premiers points. L'une d'elles contient ainsi trois nouveaux points d'inflexion, et les trois derniers points seront alors sur l'autre droite, puisque les neuf points sont communs à deux courbes du troisième degré (nº 564, corollaire III). On peut conclure de là que les douze droites considérées forment quatre systèmes de trois droites passant par les neuf points d'inflexion.

568. Pour reconnaître la loi de la distribution des neuf points d'inflexion sur les douze droites dont il vient d'être question, on peut employer avec avantage la considération des imaginaires que Galois a introduites dans la théorie des nombres. Nous désignerons les points dont il s'agit par une même lettre affectée d'un indice susceptible de prendre neuf valeurs distinctes, et nous adopterons, pour les valeurs de cet indice, les neuf racines $ai + b$ de la congruence

$$i^9 - i \equiv 0 \pmod{3}.$$

L'une de ces racines est zéro et les huit autres sont congrues aux puissances d'une racine primitive de la con-

gruence

$$i^8 - 1 \equiv 0 \pmod{3}.$$

Celle-ci a quatre racines primitives : ce sont les racines des deux congruences irréductibles

$$i^2 - i - 1 \equiv 0, \quad i^2 + i - 1 \equiv 0 \pmod{3}.$$

Nous désignerons par i une racine de la première, et l'on aura en conséquence

$$i^2 \equiv i + 1 \pmod{3},$$

d'où

$$\left.\begin{array}{ll} i^3 \equiv 2i + 1, & i^6 \equiv 2i + 2, \\ i^4 \equiv 2, & i^7 \equiv i + 2, \\ i^5 \equiv 2i, & i^8 \equiv 1, \end{array}\right\} \pmod{3}.$$

Cela posé, considérons l'un des quatre systèmes de trois droites qui passent par les neuf points d'inflexion, et attribuons aux points situés sur ces droites les indices des trois lignes respectives du tableau suivant :

$$(1) \qquad \left\{\begin{array}{lll} 0, & 1, & 2, \\ i, & i + 1, & i + 2, \\ 2i, & 2i + 1, & 2i + 2. \end{array}\right.$$

Pour former les combinaisons des indices qui répondent à l'une quelconque des neuf lignes restantes, il faut prendre trois indices appartenant respectivement aux trois lignes du précédent tableau, et, comme rien ne distingue entre eux les trois points situés sur l'une des droites du premier système, on peut supposer que les lignes verticales du tableau (1) répondent chacune à trois points situés sur la même droite. On aura donc ce deuxième système

$$(2) \qquad \left\{\begin{array}{lll} 0, & i, & 2i, \\ 1, & i + 1, & 2i + 1, \\ 2, & i + 2, & 2i + 2. \end{array}\right.$$

et, en multipliant, on a

$$\left(\frac{MA_0}{NA_0}\right)^3 = \frac{MA_{2i}.MA_{2i+1}.MA_{2i+2}}{OA_{2i}.OA_{2i+1}.OA_{2i+2}} \times \frac{OA_i.OA_{i+1}.OA_{i+2}}{NA_i.NA_{i+1}.NA_{i+2}},$$

Il est évident qu'on trouvera la même valeur pour $\left(\frac{MA_1}{NA_1}\right)^3$ et $\left(\frac{MA_2}{NA_2}\right)^3$ en appliquant le même théorème aux droites issues des points A_1 et A_2; on a donc

$$\left(\frac{MA_0}{NA_0}\right)^3 = \left(\frac{MA_1}{NA_1}\right)^3 = \left(\frac{MA_2}{NA_2}\right)^3.$$

Les points considérés étant supposés réels, la précédente égalité exige que l'on ait

$$\frac{MA_0}{NA_0} = \frac{MA_1}{NA_1} = \frac{MA_2}{NA_2},$$

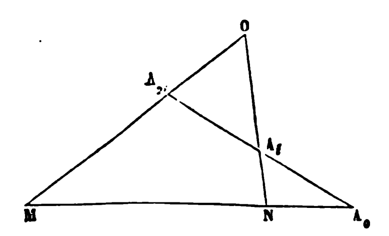
ce qui est évidemment impossible.

Cela posé, considérons le faisceau obtenu en joignant un point d'inflexion imaginaire aux autres points; l'une quelconque des quatre droites de ce faisceau coupe la courbe du troisième degré en deux points d'inflexion qui ne peuvent être réels tous les deux, ni imaginaires conjugués. L'une de ces droites contiendra le point conjugué du sommet du faisceau avec un point réel; chacune des autres contiendra au moins un nouveau point imaginaire, et, comme le nombre des points imaginaires est pair, il sera au moins égal à 6. Enfin, la droite qui passe par deux points imaginaires conjugués étant réelle, chaque couple de pareils points exige nécessairement un point d'inflexion réel, d'où il résulte qu'il y a toujours trois points d'inflexion réels et six imaginaires.

Remarque. — On pourrait faire à ce théorème l'objection que voici. On suppose que chacune des droites qui passent par deux points d'inflexion imaginaires

569. THÉORÈME IV. — *Parmi les neuf points d'inflexion d'une courbe du troisième degré réelle, il y en a toujours trois réels et six imaginaires.*

D'abord les neuf points d'inflexion ne peuvent pas être tous réels. En effet, admettons qu'ils le soient, et considérons le triangle OMN formé par les trois droites de



l'un des quatre systèmes dont nous avons établi l'existence. Supposons, par exemple, que les côtés MN, NO, OM constituent le premier système de quatre droites et que ces côtés contiennent respectivement les points

$$\begin{array}{ccc} A_0, & A_1, & A_2, \\ A_i, & A_{i+1}, & A_{i+2}, \\ A_{2i}, & A_{2i+1}, & A_{2i+2}. \end{array}$$

En appliquant la propriété connue des *transversales* au triangle OMN coupé par les trois droites issues du point A_0, savoir :

$$A_0 A_i A_{2i},\quad A_0 A_{i+1} A_{2i+2},\quad A_0 A_{i+2} A_{2i+1},$$

on trouve

$$\frac{MA_0}{NA_0}\frac{NA_i}{OA_i}\frac{OA_{2i}}{MA_{2i}} = 1,$$

$$\frac{MA_0}{NA_0}\frac{NA_{i+1}}{OA_{i+1}}\frac{OA_{2i+2}}{MA_{2i+2}} = 1,$$

$$\frac{MA_0}{NA_0}\frac{NA_{i+2}}{OA_{i+2}}\frac{OA_{2i+1}}{MA_{2i+1}} = 1,$$

formée des droites

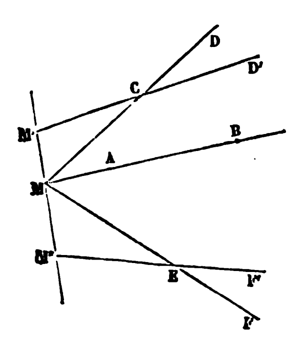
$$MAB,\ M'CD',\ M''EF';$$

d'ailleurs les points M, M', M'' sont en ligne droite : donc les six points

$$A,\ B,\ C,\ E,\ D',\ F'$$

sont sur une conique.

Cette conclusion subsiste quelle que soit la sécante MM'M''; faisons tourner celle-ci autour du point M,



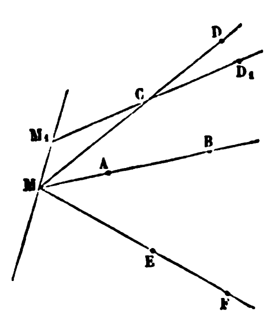
jusqu'à ce qu'elle devienne tangente à la courbe Γ. Les points M' et M'' se confondront avec M, à la limite, si celui-ci est un point d'inflexion; alors M'CD' et M''EF' viennent respectivement coïncider avec MCD et MEF. Donc les six points

$$A,\ B,\ C,\ D,\ E,\ F$$

sont sur une conique.

Mais, si M n'est pas un point d'inflexion, quand la droite MM'M'' deviendra tangente à la courbe Γ, l'un des points M', M'' seulement se confondra avec M, et l'autre point, M' par exemple, tendra vers une position limite M_1; pareillement le point F' coïncidera avec

F et le point D′ aura une certaine position limite D_1. Les six points A, B, E, F, C, D_1 sont sur une conique,



et celle-ci ne peut contenir le point D; car autrement elle aurait sept points communs avec la courbe Γ.

Corollaire I. — *Si, par un point* M *d'une courbe du troisième degré* Γ, *on mène des sécantes à cette courbe, et qu'on prenne sur chaque sécante la moyenne harmonique entre ses deux segments, les points de division ainsi obtenus seront en ligne droite, toutes les fois que* M *sera un point d'inflexion; et réciproquement, si le lieu des points harmoniques est une ligne droite, le point* M *sera un point d'inflexion de la courbe* Γ.

En effet, si M est un point d'inflexion et qu'on mène trois sécantes MAB, MCD, MEF, les points A, B, C, D, E, F sont sur une conique, et la polaire du point M, par rapport à cette conique, coupe chaque sécante en un point dont la distance à M est la moyenne harmonique des deux segments de la sécante.

Mais, si M n'est pas un point d'inflexion et qu'on mène en M la tangente MM_1, qui rencontre de nouveau la courbe en M_1, et qu'on joigne M_1C qui coupe de nouveau la courbe en D_1, les points A, B, E, F, C, D_1 seront sur une conique qui coupera la droite MC en un

point D différent de D_1. La polaire du point M par rapport à la conique coupe chaque sécante MAB, MEF, MCD′ en un point dont la distance à M est la moyenne harmonique des segments de la sécante, et il est évident que la même chose ne peut pas avoir lieu à l'égard des segments MC, MD.

Corollaire II. — *Les neuf points d'inflexion d'une courbe du troisième degré donnée sont aussi les points d'inflexion de toutes les courbes du troisième degré qui les contiennent tous.*

En effet, soit M un point d'inflexion d'une courbe du troisième degré Γ. Considérons le faisceau de quatre droites issues de M et qui renferment chacune deux nouveaux points d'inflexion. Si l'on prend, sur chaque rayon, la moyenne harmonique des segments, les quatre points de division seront en ligne droite, d'après le corollaire I, et, en raison de cette circonstance, le point M sera point d'inflexion pour chacune des courbes du troisième degré que l'on peut faire passer par les neuf points d'inflexion de la courbe donnée.

Corollaire III. — *Si u désigne une fonction entière et homogène du troisième degré de trois variables, que la caractéristique Δ représente généralement le déterminant d'une telle fonction, et que λ soit une constante quelconque donnée, on aura identiquement*

$$\Delta(\lambda u + \Delta u) = A u + B \Delta u,$$

A et B étant des constantes.

En effet, l'équation $u = 0$ représente une courbe dont les points d'inflexion sont aussi sur la courbe qui a pour équation $\Delta u = 0$. Pareillement, si l'on veut avoir les points d'inflexion de la courbe qui a pour équation

$$\lambda u + \Delta u = 0,$$

il faudra joindre à cette équation

$$\Delta(\lambda u + \Delta u) = 0;$$

or, d'après le corollaire II, celle-ci représente une courbe qui passe par les neuf points communs aux courbes $u = 0$, $\Delta u = 0$; donc son équation est de la forme

$$\mu u + \Delta u = 0 \quad \text{ou} \quad A u + B \Delta u = 0.$$

On aura par suite, identiquement,

$$\Delta(\lambda u + \Delta u) = A u + B \Delta u,$$

en déterminant convenablement les constantes A et B.

La proposition contenue dans le corollaire III est due à Hesse; le corollaire I et le théorème lui-même sont dus à M. Chasles, et c'est M. Hart qui en a tiré le premier les conséquences que nous venons de présenter (¹).

571. Théorème VI. — *Les coordonnées rectilignes de chacun des neuf points d'inflexion d'une courbe du troisième degré sont exprimables par des fonctions algébriques explicites des coefficients de l'équation de la courbe.*

En effet, soit

$$(1) \qquad u = 0$$

l'équation d'une courbe du troisième degré. Les neuf points d'inflexion de cette courbe sont aussi, comme on l'a vu, sur la courbe du troisième degré qui a pour équation

$$\Delta u = 0,$$

en sorte que, si λ désigne une constante indéterminée,

(¹) *Voir*, à ce sujet, une Note de M. Salmon, insérée dans le tome XXXIX du *Journal de Crelle*, p. 365.

l'équation

$$(2) \qquad \lambda u + \Delta u = 0$$

représentera généralement toutes les courbes du troisième degré qui passent par les neuf points d'inflexion de la proposée. Or nous avons vu qu'on peut faire passer par ces neuf points quatre lignes du troisième degré formées chacune de trois droites ; donc il y a quatre valeurs de λ pour lesquelles l'équation (2) se décompose en facteurs linéaires. En outre, d'après le corollaire III du précédent théorème, on a identiquement

$$\Delta(\lambda u + \Delta u) = \mathrm{A}u + \mathrm{B}\Delta u,$$

A et B étant évidemment des fonctions entières de λ du troisième degré. Or, si l'équation $\lambda u + \Delta u = 0$ représente trois droites, l'équation $\Delta(\lambda u + \Delta u) = 0$ ou $\mathrm{A}u + \mathrm{B}\Delta u = 0$ représentera aussi les mêmes droites (n° 560); donc, dans cette hypothèse, on a

$$(3) \qquad \mathrm{A} - \lambda \mathrm{B} = 0\ ([1]).$$

Si l'on résout cette équation du quatrième degré en λ, que l'on prenne pour λ l'une quelconque de ces racines et qu'ensuite on résolve l'équation (2) par rapport à l'une des coordonnées, on trouvera nécessairement que les trois valeurs de cette coordonnée sont des fonctions linéaires de la deuxième coordonnée. La décomposition de l'équation (2) en facteurs linéaires étant ainsi effectuée, on aura les équations de trois droites contenant chacune trois des neuf points d'inflexion de

---

([1]) Dans un beau Mémoire publié au tome XXXIX du *Journal de Crelle*, M. Aronhold a obtenu effectivement cette équation du quatrième degré en λ sous une forme bien remarquable. Car les coefficients s'expriment par deux fonctions seulement des coefficients de l'équation de la courbe proposée.

la proposée, et, pour avoir les coordonnées de ces neuf points, il suffira de chercher successivement les solutions communes à l'équation (1) et à l'équation de chacune des trois droites, ce qui exigera seulement la résolution de trois équations du troisième degré à une inconnue.

Il s'ensuit que les coordonnées des neuf points d'inflexion sont exprimables par des fonctions algébriques explicites des coefficients de l'équation proposée.

Corollaire. — *L'équation du neuvième degré qui a pour racines les abscisses des points d'inflexion d'une courbe du troisième degré est toujours résoluble algébriquement.*

Sur un théorème de Steiner relatif aux courbes du troisième degré.

572. Si u désigne une fonction homogène du degré n des trois variables x, y, z, l'équation

$$(1) \qquad u = 0$$

représentera une courbe du degré n dont les coordonnées seront $\frac{x}{z}$, $\frac{y}{z}$.

L'équation de la tangente en un point (x, y, z) de la courbe (1) est

$$\left(\frac{X}{Z} - \frac{x}{z}\right)\frac{du}{dx} + \left(\frac{Y}{Z} - \frac{y}{z}\right)\frac{du}{dy} = 0;$$

si l'on ajoute le terme

$$\left(\frac{Z}{Z} - \frac{z}{z}\right)\frac{du}{dz},$$

qui est identiquement nul, la précédente équation pren-

dra la forme

$$(2) \qquad X\frac{du}{dx}+Y\frac{du}{dy}+Z\frac{du}{dz}=0,$$

à cause de

$$x\frac{du}{dx}+y\frac{du}{dy}+z\frac{du}{dz}=nu=0.$$

Si les quantités X, Y, Z se rapportent à un point donné M, l'équation (2) représentera une courbe du degré $n-1$, et cette courbe coupera la proposée en $n(n-1)$ points. Il s'ensuit que, par le point donné M, on peut mener en général $n(n-1)$ tangentes à la courbe (1).

Dans le cas de $n=2$, l'équation (2) représente une ligne droite qui est la polaire du point M par rapport à la conique (1); cette équation (2) ne change pas quand on remplace X, Y, Z par x, y, z, et inversement. En effet, si l'on pose, comme au n° 558,

$$\frac{d^2u}{dx^2}=u_{1,1},\quad \frac{d^2u}{dy^2}=u_{2,2},\quad \frac{d^2u}{dz^2}=u_{3,3},$$
$$\frac{d^2u}{dy\,dz}=u_{2,3},\quad \frac{d^2u}{dx\,dz}=u_{1,3},\quad \frac{d^2u}{dx\,dy}=u_{1,2},$$

on aura, dans le cas de $n=2$,

$$\frac{du}{dx}=xu_{1,1}+yu_{1,2}+zu_{1,3},$$
$$\frac{du}{dy}=xu_{2,1}+yu_{2,2}+zu_{2,3},$$
$$\frac{du}{dz}=xu_{3,1}+yu_{3,2}+zu_{3,3},$$

et, comme les quantités $u_{1,1}$, $u_{1,2}$, ... sont ici des constantes, il suffit de substituer les expressions précédentes dans l'équation (2), pour justifier notre assertion.

573. Considérons maintenant le cas de $n = 3$; l'équation (2) représentera une conique qui déterminera sur la courbe proposée les points de contact des six tangentes qu'on peut lui mener par le point donné. Pour abréger, je représenterai cette équation (2) par

$$v = 0,$$

et le centre de la conique sera déterminé par les équations

$$\frac{dv}{dx} = 0, \quad \frac{dv}{dy} = 0.$$

D'après cela, si l'on veut avoir la condition pour que la conique (2) se réduise au système de deux droites, il suffira d'exprimer que les trois équations précédentes sont satisfaites par les mêmes valeurs de x et de y. Or les dernières équations réduisent $v = 0$ à $\frac{dv}{dz} = 0$; donc la condition demandée s'obtiendra en éliminant x et y entre les trois équations du premier degré

$$\frac{dv}{dx} = 0, \quad \frac{dv}{dy} = 0, \quad \frac{dv}{dz} = 0.$$

Ces équations se déduisent de l'équation (2) en remplaçant dans celle-ci u par $\frac{du}{dx}$, $\frac{du}{dy}$, $\frac{du}{dz}$, successivement; donc, d'après ce qui a été dit plus haut, elles ne changeront pas si l'on y remplace X, Y, Z par x, y, z, et inversement. On pourra ainsi leur donner cette forme :

$$(3) \qquad \begin{cases} xU_{1,1} + yU_{1,2} + zU_{1,3} = 0, \\ xU_{2,1} + yU_{2,2} + zU_{2,3} = 0, \\ xU_{3,1} + yU_{3,2} + zU_{3,3} = 0, \end{cases}$$

en représentant par U, $U_{1,1}$, $U_{1,2}$, ... ce que deviennent u, $u_{1,1}$, $u_{1,2}$, ... quand on écrit X, Y, Z au lieu de x, y, z.

Maintenant l'élimination de x et de y entre les équations (3) donne

$$(4) \qquad \Delta U = 0,$$

ΔU étant le déterminant de U; on a ainsi ce théorème :

THÉORÈME I. — *Soient u une fonction entière et homogène du troisième degré des variables x, y, z, et Δu le déterminant de u. Soient aussi* U *et* ΔU *ce que deviennent u et Δu quand on écrit* X, Y, Z *au lieu de x, y, z. Pour que les points de contact des six tangentes menées à la courbe $u = 0$ par le point* (X, Y, Z) *soient situés sur deux droites, il faut et il suffit que l'on ait*

$$\Delta U = 0.$$

Et il en résulte cette conséquence importante :

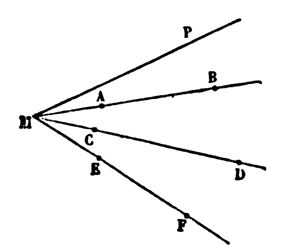
COROLLAIRE. — *Par un point d'inflexion d'une courbe du troisième degré on peut mener à cette courbe trois tangentes indépendamment de celle qui touche la courbe au point d'inflexion, et les points de contact de la courbe avec ces trois tangentes sont en ligne droite.*

574. Les considérations qui précèdent nous permettent d'établir le théorème suivant, que Steiner a publié sans démonstration dans le tome XI du *Journal de Mathématiques pures et appliquées.*

THÉORÈME II. — *Une courbe du troisième degré contient en général 27 points en chacun desquels elle peut avoir un contact du cinquième ordre avec une conique. L'équation du vingt-septième degré qui détermine ces 27 points est toujours résoluble algébriquement.*

En effet, soit P un point de la courbe donnée; menons PM tangente à la courbe en P, et rencontrant de nouveau celle-ci en M. Menons enfin, par le point M,

trois sécantes qui rencontrent la courbe aux points A et B, C et D, E et F respectivement.



Si le point M est un point d'inflexion, les six points A, B, C, D, E, F seront sur une conique (n° 570), et si l'on fait varier ces sécantes de manière qu'elles tendent toutes les trois vers la limite MP, la conique variera, et, à la limite, elle aura, avec la courbe donnée, six points communs confondus en un seul; il y aura donc en P contact du cinquième ordre.

Mais, si le point M n'est pas un point d'inflexion, la conique déterminée par les cinq points B, C, D, E, F ne passera pas par le point A, quelque voisine de MP que soit MAB, et elle coupera la courbe donnée en un sixième point A'; donc, quand on arrivera à la limite, la conique deviendra osculatrice en P à la courbe donnée, comme dans le premier cas; mais elle coupera celle-ci en un nouveau point, et elle aura seulement avec elle un contact du quatrième ordre.

Il résulte de là que les points P, qui possèdent la propriété contenue dans l'énoncé du théorème, sont les points de contact des tangentes menées à la courbe donnée par ses divers points d'inflexion; et puisque, par chaque point d'inflexion, on peut mener trois tangentes, le nombre total des points P est 3×9 ou 27.

Enfin, les coordonnées des points d'inflexion sont

exprimables par des fonctions algébriques explicites des coefficients de l'équation qui représente la courbe donnée; en outre, la détermination des trois points P qui répondent au même point M dépend seulement d'une équation du troisième degré. Donc l'équation du vingt-septième degré, dont dépend la recherche des 27 points P, est toujours résoluble algébriquement.

Propriété de l'équation du neuvième degré qui a pour racines les abscisses des points d'inflexion d'une courbe du troisième degré.

575. Soit

$$(1) \qquad u = 0$$

l'équation d'une courbe du troisième degré entre les coordonnées rectilignes $\frac{x}{z}$ et $\frac{y}{z}$; nous avons vu que les points d'inflexion de cette courbe sont sur une seconde courbe du troisième degré,

$$(2) \qquad \Delta u = 0.$$

Si l'on élimine y entre les équations (1) et (2), on obtient une équation

$$(3) \qquad v = 0,$$

homogène par rapport à x et z et du neuvième degré. Cette équation, dont les racines $\frac{x}{z}$ représentent les abscisses des points d'inflexion, est toujours résoluble algébriquement, comme nous l'avons démontré plus haut. Mais il existe, entre les racines de l'équation (3), des relations remarquables que nous allons faire connaître,

d'après Hesse, et desquelles ce géomètre a déduit la résolubilité par radicaux de l'équation (3).

Remarquons d'abord que la valeur de $\frac{y}{z}$ correspondant à chaque racine $\frac{x}{z}$ de l'équation (3) peut s'exprimer en fonction rationnelle de $\frac{x}{z}$ et des quantités connues de l'équation (1). Cela résulte immédiatement de la méthode que nous avons exposée au n° 73 pour la résolution de deux équations simultanées. D'après cela, les coordonnées de chaque point d'inflexion de la courbe proposée doivent satisfaire à une même équation de la forme

$$(4) \qquad \frac{y}{z} = \mathrm{F}\left(\frac{x}{z}\right),$$

où F désigne une fonction rationnelle.

Soient maintenant $\frac{x_0}{z_0}$, $\frac{y_0}{z_0}$ et $\frac{x_1}{z_1}$, $\frac{y_1}{z_1}$ les coordonnées de deux points d'inflexion de la courbe (1); la droite qui passe par ces deux points aura pour équation

$$\frac{\frac{x}{z} - \frac{x_0}{z_0}}{\frac{x}{z} - \frac{x_1}{z_1}} = \frac{\frac{y}{z} - \frac{y_0}{z_0}}{\frac{y}{z} - \frac{y_1}{z_1}}.$$

En désignant par $-\lambda \frac{z_1}{z_0}$ la valeur commune des deux membres, il vient

$$\frac{x}{z}(z_0 + \lambda z_1) = x_0 + \lambda x_1,$$

$$\frac{y}{z}(z_0 + \lambda z_1) = y_0 + \lambda y_1.$$

on peut disposer de z de manière que l'on ait $z = z_0 + \lambda z_1$, et l'on voit alors que notre droite pourra être représentée par les trois équations suivantes :

$$(5) \qquad x = x_0 + \lambda x_1, \quad y = y_0 + \lambda y_1, \quad z = z_0 + \lambda z_1.$$

Au moyen de ces équations, on obtiendra tous les points de la droite en donnant à λ toutes les valeurs possibles. Or, d'après le théorème de Maclaurin démontré au n° 566, cette droite coupe la courbe (1) en un troisième point d'inflexion ; pour avoir la valeur de λ qui convient à ce troisième point, il suffit de porter dans l'équation (1) les valeurs de x, y, z tirées des équations (5), et de résoudre ensuite l'équation obtenue ainsi, par rapport à λ. Par cette substitution il vient

$$(6)\left\{\begin{aligned} &(u)_0 + \lambda\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right] \\ &\quad + \lambda^2\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] + \lambda^3 (u)_1 = 0, \end{aligned}\right.$$

les indices 0 et 1 indiquant que, dans les expressions qui en sont affectées, on doit mettre x_0, y_0, z_0 ou x_1, y_1, z_1 à la place de x, y, z. En effet, il résulte immédiatement de la formule de Taylor qu'après la substitution les deux premiers termes de u sont

$$(u)_0 + \lambda\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right],$$

et il est évident que les deux derniers termes doivent se déduire de ces deux-ci, en changeant $x_0, y_0, z_0, x_1, y_1, z_1$ en $\lambda x_1, \lambda y_1, \lambda z_1, \frac{1}{\lambda} x_0, \frac{1}{\lambda} y_0, \frac{1}{\lambda} z_0$.

Si l'on supprime les termes $(u)_0$ et $(u)_1$ qui sont nuls, l'équation (6), divisée par λ, donne la valeur sui-

vante de λ :

$$(7)\qquad \lambda = -\frac{x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0}{x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1},$$

qui convient au troisième point d'inflexion. Si l'on désigne par $\frac{x_2}{z_2}$, $\frac{y_2}{z_2}$ les coordonnées de ce point, et qu'on porte la valeur de λ, que nous venons de trouver, dans les équations (5), on aura

$$= \frac{x_0\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] - x_1\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right]}{z_0\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] - z_1\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right]},$$

$$= \frac{y_0\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] - y_1\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right]}{z_0\left[x_0\left(\frac{du}{dx}\right)_1 + y_0\left(\frac{du}{dy}\right)_1 + z_0\left(\frac{du}{dz}\right)_1\right] - z_1\left[x_1\left(\frac{du}{dx}\right)_0 + y_1\left(\frac{du}{dy}\right)_0 + z_1\left(\frac{du}{dz}\right)_0\right]},$$

Considérons, en particulier, la première de ces équations : le second membre ne change pas quand on change x_0, y_0, z_0 en x_1, y_1, z_1, et réciproquement; en divisant le numérateur et le dénominateur de ce second membre par $z_0^2 z_1^2$, il prend la forme

$$f\left(\frac{x_0}{z_0}, \frac{y_0}{z_0}, \frac{x_1}{z_1}, \frac{y_1}{z_1}\right),$$

f désignant une fonction rationnelle qui ne change pas quand on transpose les indices 0 et 1. Or, d'après l'équation (4), on a

$$\frac{y_0}{z_0} = \mathrm{F}\left(\frac{x_0}{z_0}\right), \quad \frac{y_1}{z_1} = \mathrm{F}\left(\frac{x_1}{z_1}\right),$$

F désignant une fonction rationnelle. Donc la valeur

de $\frac{x_2}{z_2}$ peut se réduire à la forme suivante :

$$\frac{x_2}{z_2} = \theta\left(\frac{x_0}{z_0}, \frac{x_1}{z_1}\right),$$

θ désignant une fonction rationnelle et symétrique des deux quantités qu'elle renferme. Il est évident que l'équation précédente ne cessera pas d'être exacte si l'on exécute une substitution sur les indices 0, 1, 2; car on serait arrivé directement aux équations qu'on obtient par les substitutions, en partant du premier point d'inflexion et du troisième, ou du deuxième et du troisième. au lieu de partir du premier et du deuxième. Donc les abscisses $\frac{x_0}{z_0}, \frac{x_1}{z_1}, \frac{x_2}{z_2}$ de trois points d'inflexion en ligne droite satisfont aux trois relations

$$\frac{x_0}{z_0} = \theta\left(\frac{x_1}{z_1}, \frac{x_2}{z_2}\right), \quad \frac{x_1}{z_1} = \theta\left(\frac{x_2}{z_2}, \frac{x_0}{z_0}\right), \quad \frac{x_2}{z_2} = \theta\left(\frac{x_0}{z_0}, \frac{x_1}{z_1}\right),$$

où θ, nous le répétons, désigne une fonction rationnelle et symétrique. De cette propriété résulte, comme on va le voir, la résolubilité de l'équation (3).

Sur la résolution algébrique d'une classe d'équations du neuvième degré.

576. Il était intéressant de chercher à rattacher la question particulière dont nous venons de nous occuper à une théorie plus générale; c'est ce qu'a fait très-heureusement Hesse en établissant le théorème suivant :

Théorème. — *Soient*

(1) $$\chi(x) = 0$$

une équation du neuvième degré et θ une fonction ra-

tionnelle et symétrique donnée de deux variables. Si l'équation proposée a cette propriété, que deux racines quelconques x_λ et x_μ fournissent une troisième racine x_κ, de telle sorte qu'on ait en même temps

$$(2)\quad x_\kappa = \theta(x_\lambda, x_\mu),\quad x_\lambda = \theta(x_\mu, x_\kappa),\quad x_\mu = \theta(x_\kappa, x_\lambda),$$

cette équation sera résoluble algébriquement.

On voit que l'équation qui a pour racines les abscisses des points d'inflexion d'une courbe du troisième degré a la propriété dont il s'agit ici.

Hesse nomme *racines conjuguées* trois racines de l'équation (1) qui satisfont aux relations (2). Il est évident que chaque racine fait partie de quatre combinaisons de trois racines conjuguées; par suite, en comptant quatre combinaisons pour chaque racine, on aurait 4×9 ou trente-six combinaisons; mais, chacune de ces combinaisons se trouvant répétée trois fois, on voit qu'il n'y a que douze combinaisons distinctes de racines conjuguées. Et, comme le nombre total des combinaisons de trois racines est 84, il y a soixante-douze combinaisons de trois racines non conjuguées.

Considérons l'un quelconque des quatre groupes de racines conjuguées, et désignons-le par

$$x_\kappa x_\lambda x_\mu,\quad x_{\kappa'} x_{\lambda'} x_{\mu'},\quad x_{\kappa''} x_{\lambda''} x_{\mu''}.$$

On peut supposer que x_κ, $x_{\kappa'}$, $x_{\kappa''}$ ne soient point conjuguées, et, par suite, on pourra les considérer comme trois racines *quelconques* non conjuguées. Alors, comme rien ne distingue entre eux les indices λ et μ, λ' et μ', λ'' et μ'', on aura ces trois combinaisons de racines conjuguées,

$$x_{\kappa'} x_{\kappa''} x_\lambda,\quad x_{\kappa''} x_\kappa x_{\lambda'},\quad x_\kappa x_{\kappa'} x_{\lambda''};$$

les six autres combinaisons de racines conjuguées sont

alors nécessairement

$$x_\varkappa x_{\mu'} x_{\mu''},\quad x_{\varkappa'} x_{\mu''} x_\mu,\quad x_{\varkappa''} x_\mu x_{\mu'};$$

$$x_{\lambda'} x_{\lambda''} x_\mu,\quad x_{\lambda''} x_\lambda x_{\mu'},\quad x_\lambda x_{\lambda'} x_{\mu''}.$$

On voit que les neuf racines sont exprimables en fonction rationnelle de trois racines non conjuguées quelconques $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$; on a effectivement

$$(3)\quad \begin{cases} x_\varkappa = x_\varkappa, & x_\lambda = \theta(x_{\varkappa'}, x_{\varkappa''}), & x_\mu = \theta[\theta(x_{\varkappa''}, x_\varkappa), \theta(x_\varkappa, x_{\varkappa'})], \\ x_{\varkappa'} = x_{\varkappa'}, & x_{\lambda'} = \theta(x_{\varkappa''}, x_\varkappa), & x_{\mu'} = \theta[\theta(x_\varkappa, x_{\varkappa'}), \theta(x_{\varkappa'}, x_{\varkappa''})], \\ x_{\varkappa''} = x_{\varkappa''}, & x_{\lambda''} = \theta(x_\varkappa, x_{\varkappa'}), & x_{\mu''} = \theta[\theta(x_{\varkappa'}, x_{\varkappa''}), \theta(x_{\varkappa''}, x_\varkappa)]. \end{cases}$$

Cela posé, désignons par α une constante indéterminée, et formons la fonction symétrique suivante de trois racines conjuguées quelconques $x_\varkappa$, x_λ, x_μ du troisième degré par rapport à α, savoir :

$$(4)\qquad y_{\varkappa,\lambda,\mu} = (\alpha - x_\varkappa)(\alpha - x_\lambda)(\alpha - x_\mu);$$

en remplaçant $x_\varkappa$, x_λ, x_μ par chacune des douze combinaisons de racines conjuguées, on obtiendra les douze valeurs distinctes de la fonction $y_{\varkappa,\lambda,\mu}$.

Formons ensuite la fonction symétrique suivante :

$$(5)\qquad z = (6 - y_{\varkappa,\lambda,\mu})(6 - y_{\varkappa',\lambda',\mu'})(6 - y_{\varkappa'',\lambda'',\mu''}),$$

qui est du troisième degré par rapport à l'indéterminée 6. Soient z_0, z_1, z_2, z_3 les quatre valeurs que prend z quand on y met successivement, pour $y_{\varkappa,\lambda,\mu}$, $y_{\varkappa',\lambda',\mu'}$, $y_{\varkappa'',\lambda'',\mu''}$, les quatre groupes de valeurs qui conviennent à ces quantités. Formons enfin l'équation du quatrième degré

$$(6)\qquad z^4 + A_1 z^3 + A_2 z^2 + A_3 z + A_4 = 0,$$

qui a pour racines z_0, z_1, z_2, z_3.

Je dis que les coefficients de l'équation (6) sont exprimables rationnellement en fonction des quantités connues de l'équation (1) et de la fonction θ. En effet, on a

$$(7)\quad \begin{cases} y_{\varkappa,\lambda,\mu} = (\alpha - x_\varkappa)\ (\alpha - x_\lambda)\ (\alpha - x_\mu), \\ y_{\varkappa',\lambda',\mu'} = (\alpha - x_{\varkappa'})\ (\alpha - x_{\lambda'})\ (\alpha - x_{\mu'}), \\ y_{\varkappa'',\lambda'',\mu''} = (\alpha - x_{\varkappa''})\ (\alpha - x_{\lambda''})\ (\alpha - x_{\mu''}); \end{cases}$$

en portant ces valeurs dans la formule (5) et en se servant des formules (4), on aura la valeur de z exprimée en fonction rationnelle de trois racines non conjuguées $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$, savoir :

$$(8)\qquad z = \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''}),$$

et cette fonction ψ sera symétrique par rapport à $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$; car il est aisé de voir, d'après les formules (3), qu'en permutant ces trois racines les quantités $y_{\varkappa,\lambda,\mu}$, $y_{\varkappa',\lambda',\mu'}$, $y_{\varkappa'',\lambda'',\mu''}$ ne font que se changer les unes dans les autres, ce qui ne change pas la valeur de z.

Élevons le second membre de l'équation (8) à une puissance entière quelconque de degré m; désignons par

$$\sum\nolimits'' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

la somme des termes qu'on déduit de $\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$ en prenant successivement pour $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ les soixante-douze combinaisons de trois racines non conjuguées; par

$$\sum\nolimits' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

la somme des termes qu'on déduit de $\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$ en prenant successivement pour $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ les douze com-

binaisons de racines conjuguées; enfin par

$$\sum \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

la somme de tous les termes qu'on déduit de $\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$ en prenant pour $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ toutes les quatre-vingt-quatre combinaisons de trois racines. On aura

$$(9)\quad \sum\nolimits'' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m + \sum\nolimits' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m = \sum \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m.$$

Le second membre de cette formule (9) est une fonction rationnelle et symétrique de toutes les racines, et l'on peut, par conséquent, l'exprimer en fonction rationnelle des quantités connues. Il en est de même de $\sum' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$; en effet, $x_\varkappa$, $x_{\varkappa'}$, $x_{\varkappa''}$ étant des racines conjuguées, on a

$$\psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m = \psi[x_\varkappa, x_{\varkappa'}, \theta(x_\varkappa, x_{\varkappa'})]^m = \psi[x_{\varkappa'}, x_{\varkappa''}, \theta(x_{\varkappa'}, x_{\varkappa''})]^m$$
$$= \psi[x_{\varkappa''}, x_\varkappa, \theta(x_{\varkappa''}, x_\varkappa)]^m;$$

d'où il suit que

$$\sum\nolimits' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m$$

est égale au tiers de la somme des trente-six valeurs que prend

$$\psi[x_\varkappa, x_{\varkappa'}, \theta(x_\varkappa, x_{\varkappa'})]^m$$

quand on prend pour $x_\varkappa$, $x_{\varkappa'}$ les trente-six combinaisons de deux racines. En désignant cette somme par le signe $\sum$, on a

$$(10)\quad \sum\nolimits' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m = \frac{1}{3} \sum \psi[x_\varkappa, x_{\varkappa'}, \theta(x_\varkappa, x_{\varkappa'})]^m,$$

et, par suite,

$$(11)\quad \left\{\begin{aligned} &\sum{}'' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m \\ &= \sum \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m - \frac{1}{3}\sum \psi[x_\varkappa, x_{\varkappa'}, \theta(x_\varkappa, x_{\varkappa'})]^m, \end{aligned}\right.$$

ce qui montre que $\sum'' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})$ est une fonction rationnelle et symétrique de toutes les racines; on peut donc l'exprimer, en fonction rationnelle des quantités connues. Si maintenant on remarque qu'aux soixante-douze combinaisons de racines non conjuguées répondent seulement quatre valeurs de la fonction z^m, savoir : z_0^m, z_1^m, z_2^m, z_3^m, et que chacune de ces valeurs revient dix-huit fois, on verra que l'on a

$$(12)\qquad z_0^m + z_1^m + z_2^m + z_3^m = \frac{1}{18}\sum{}'' \psi(x_\varkappa, x_{\varkappa'}, x_{\varkappa''})^m.$$

En donnant au nombre m les valeurs 1, 2, 3, 4, on obtiendra, par la formule (12), les sommes de puissances semblables des racines de l'équation (6) qui sont nécessaire pour calculer les coefficients A_1, A_2, A_3, A_4; on voit que ces coefficients se trouvent ainsi exprimés en fonction rationnelle des quantités connues.

Voici maintenant comment on obtiendra les racines de l'équation (1). On cherchera une racine quelconque de l'équation (6). Cette racine sera, d'après ce qui précède, une fonction entière et du troisième degré de l'indéterminée θ; en égalant à zéro cette racine, on aura une équation du troisième degré en θ dont les racines seront les trois quantités qui forment l'un des quatre groupes dans lesquels se partagent les douze quantités $y_{\varkappa,\lambda,\mu}$. En égalant à zéro une de ces nouvelles racines,

on aura une équation du troisième degré par rapport à l'indéterminée α ; les trois valeurs de α racines de cette équation seront trois racines conjuguées de l'équation (1). Pour avoir toutes les racines de l'équation (1), il suffit d'opérer de la même manière avec chacune des racines de l'équation (6).

CHAPITRE V.

SUR LES ÉQUATIONS RÉSOLUBLES ALGÉBRIQUEMENT.

Recherches de Galois. Théorèmes généraux.

577. L'analyse que nous avons développée dans les deux Chapitres précédents nous a conduit à la résolution algébrique de certaines classes d'équations. Mais ces équations si remarquables sont-elles les seules qui soient susceptibles d'une telle résolution? Quelles sont, en d'autres termes, les équations résolubles? Telle est la question qui vient se poser naturellement et à laquelle Abel et Galois ont les premiers attaché leur nom.

Je me propose d'exposer ici la théorie contenue dans le Mémoire de Galois intitulé : *Sur les conditions de résolubilité des équations par radicaux;* ce Mémoire a été publié pour la première fois en 1846, dans le tome XI du *Journal de Mathématiques pures et appliquées,* quinze ans après la mort de l'illustre auteur. J'ai suivi l'ordre des propositions que Galois avait adopté, mais j'ai dû le plus souvent suppléer à l'insuffisance des démonstrations.

Nous avons défini avec précision (nos 100 et 527) le sens qu'on doit attacher, dans chaque cas, aux dénominations de *diviseur rationnel d'une fonction entière,* et généralement de *quantité rationnelle,* ainsi qu'à celles de *fonction irréductible* et d'*équation irréductible.* Nous avons dit aussi qu'une équation irréductible donnée peut devenir réductible, lorsque l'on admet à figurer.

parmi les quantités connues, certaines quantités qui n'étaient pas d'abord regardées comme telles.

En général, quand nous conviendrons de regarder comme connue une certaine irrationnelle, par exemple une racine d'une fonction rationnelle des quantités connues, nous dirons avec Galois que nous ***adjoignons*** cette quantité à l'équation proposée. En d'autres termes, la quantité dont il s'agit sera dite ***adjointe à l'équation***. Alors une quantité sera ***rationnelle***, si elle peut s'exprimer par une fonction rationnelle des quantités primitivement connues et des quantités adjointes. Ainsi l'équation

$$x^4 + x^3 - 4x^2 - 4x + 1 = 0,$$

dont dépend la division du cercle en quinze parties égales, est actuellement irréductible, parce que les quantités regardées comme connues sont ici les seuls nombres rationnels; mais elle deviendra réductible, si on lui adjoint une racine de l'équation

$$z^2 - 5 = 0,$$

c'est-à-dire si on lui adjoint le radical $\sqrt{5}$; effectivement son premier membre est le produit des deux facteurs

$$x^2 + \frac{1+\sqrt{5}}{2}x - \left(\frac{-1+\sqrt{5}}{2}\right)^2,$$
$$x^2 - \frac{-1+\sqrt{5}}{2}x - \left(\frac{1+\sqrt{5}}{2}\right)^2,$$

lesquels sont rationnels, après l'adjonction dont il vient d'être question.

Les recherches de Galois reposent sur les propositions démontrées aux nos 502 et 504, qui acquièrent ainsi une importance considérable, et sur les propriétés des systèmes de substitutions conjuguées. Galois em-

ploie la considération des groupes de permutations dont nous avons parlé aux n°s 442 et 443, mais il nous a paru préférable de nous en tenir aux substitutions. Au reste, ce n'est là qu'un simple changement dans la forme des énoncés des théorèmes, car il n'y a lieu de considérer les permutations qu'au point de vue des substitutions par lesquels on passe des unes aux autres.

578. Théorème I. — *Soit*

$$f(x) = 0 \tag{1}$$

une équation de degré n dont les n racines

$$x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1} \tag{2}$$

sont inégales. Il existe toujours un système de substitutions conjuguées G *jouissant de la double propriété suivante :*

1° *Que toute fonction rationnelle des racines dont la valeur numérique est invariable par les substitutions de* G *soit exprimable en fonction rationnelle des quantités connues ;*

2° *Réciproquement, que toute fonction rationnelle des racines, exprimable rationnellement par les quantités connues, conserve la même valeur numérique quand on lui applique toutes les substitutions de* G.

Il est bien entendu que, dans cet énoncé, nous comprenons parmi les quantités connues celles qui ont pu être adjointes à l'équation.

Soit V une fonction rationnelle des racines (2) telle, que les

$$N = 1.2\ldots n$$

fonctions qu'on en déduit, par les substitutions, aient des valeurs numériques inégales ; par exemple, on pourra faire

$$V = \alpha_0 x_0 + \alpha_1 x_1 + \ldots + \alpha_{n-1} x_{n-1},$$

$\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ étant des nombres entiers convenablement choisis. Soient encore

$$\mathcal{F}(V) = 0$$

l'équation du degré N qui a pour racines les N valeurs de V, et F(V) un diviseur irréductible, d'un certain degré ν, du polynôme $\mathcal{F}(V)$. Désignons enfin les ν racines de l'équation

$$(3) \qquad F(V) = 0$$

par

$$(4) \qquad V_0, V_1, V_2, \ldots, V_{\nu-1}.$$

D'après le théorème du n° 504, les n racines x de l'équation (1) pourront être représentées par l'une quelconque des lignes horizontales du tableau

$$(5) \quad \left\{ \begin{array}{lllll} \psi_0(V_0), & \psi_1(V_0), & \psi_2(V_0), & \ldots, & \psi_{n-1}(V_0), \\ \psi_0(V_1), & \psi_1(V_1), & \psi_2(V_1), & \ldots, & \psi_{n-1}(V_1), \\ \ldots\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ \psi_0(V_{\nu-1}), & \psi_1(V_{\nu-1}), & \psi_2(V_{\nu-1}), & \ldots, & \psi_{n-1}(V_{\nu-1}), \end{array} \right.$$

$\psi_0(V), \psi_1(V), \ldots$ étant des fonctions rationnelles de V et des quantités connues. Le tableau (5) renferme ainsi ν permutations des racines x, et nous avons démontré au n° 504 que ces permutations forment un groupe, c'est-à-dire que les substitutions

$$(6) \qquad 1, S_1, S_2, \ldots, S_{\nu-1},$$

par lesquelles on obtient les ν permutations (5) au moyen de la première d'entre elles, constituent un système conjugué G. Je dis que ce système G jouit de la double propriété énoncée.

En effet, désignons par Ω une fonction rationnelle

des racines (2) et posons

$$\Omega = \Phi[\psi_0(V_0), \psi_1(V_0), \ldots, \psi_{n-1}(V_0)],$$

Ω sera une fonction rationnelle de V_0, et l'on pourra écrire

$$(7) \qquad \Omega = \Psi(V_0),$$

Ψ étant une fonction rationnelle.

Cela posé, supposons d'abord que la valeur numérique de Ω ne soit pas changée par les substitutions (6) du système G; comme ces substitutions peuvent s'effectuer en remplaçant successivement V_0 par chacune des valeurs (4), on aura

$$\Omega = \Psi(V_0) = \Psi(V_1) = \ldots = \Psi(V_{\nu-1}),$$

et, par suite,

$$\Omega = \frac{1}{\nu}[\Psi(V_0) + \Psi(V_1) + \ldots + \Psi(V_{\nu-1})];$$

le second membre de cette formule est une fonction symétrique des racines de l'équation (3); donc Ω est exprimable en fonction rationnelle des quantités connues.

Pour démontrer la réciproque, supposons que Ω soit exprimable en fonction rationnelle des quantités connues. Alors, d'après la formule (7), V_0 sera l'une des racines de l'équation

$$\Psi(V) - \Omega = 0;$$

mais, comme V_0 est racine de l'équation (3) que nous supposons irréductible, toutes les racines de cette équation (3) doivent satisfaire à l'équation précédente, et l'on a en conséquence

$$\Omega = \Psi(V_0) = \Psi(V_1) = \ldots = \Psi(V_{\nu-1});$$

la valeur numérique de Ω est donc invariable par les

substitutions de G, ce qui achève la démonstration du théorème énoncé.

Pour abréger le discours, je donnerai le nom de *fonction résolvante* à la fonction V, et l'équation irréductible (3) sera dite *équation résolvante*.

579. Théorème II. — *Toute substitution qui jouit de la double propriété mentionnée dans l'énoncé du précédent théorème appartient au système conjugué dont ce théorème établit l'existence.*

Conservons toutes les notations dont nous avons fait usage dans la démonstration du théorème I, et désignons par X une fonction des n racines $x_0, x_1, \ldots, x_{n-1}$ qui prenne par les substitutions les $N = 1.2.3\ldots n$ valeurs

$$X_0,\ X_1,\ X_2,\ \ldots,\ X_{N-1}$$

numériquement distinctes. Soient aussi

$$X_0,\ X_1,\ X_2,\ \ldots,\ X_{\nu-1}$$

les ν valeurs que prend X quand on lui applique les ν substitutions de G, et posons

$$\Omega = (X - X_0)(X - X_1)\ldots(X - X_{\nu-1}),$$

X désignant ici une indéterminée. La valeur de la fonction Ω est invariable par les substitutions de G; elle est donc exprimable rationnellement en fonction des quantités connues, d'après le théorème I. D'ailleurs, il est évident que la valeur de Ω changera si l'on applique à cette fonction une substitution T non comprise dans le système G; donc la substitution T n'a pas les propriétés des substitutions de G qui font l'objet du théorème I.

Ainsi les substitutions de G jouissent, à l'égard de l'équation proposée, d'une propriété qui leur appartient

exclusivement; je nommerai ce système le *système conjugué propre à l'équation* ([1]).

580. Théorème III. — *Soit* G *le système conjugué propre à une équation donnée de degré n*

$$(1) \qquad f(x) = 0,$$

à laquelle plusieurs irrationnelles peuvent avoir été adjointes. Si l'on adjoint à cette équation une racine z_0 *d'une équation auxiliaire irréductible de degré m*

$$(2) \qquad \varphi(z) = 0,$$

dont les coefficients sont rationnellement connus, et qu'après cette adjonction le système conjugué Γ *propre à l'équation* (1) *ne renferme qu'une partie des substitutions de* G, *auquel cas l'ordre de* Γ *sera un sous-multiple de l'ordre de* G, *les* $m = pq$ *racines de l'équation* (2) *se partageront en un certain nombre p de groupes composés chacun de q racines, savoir :*

$$\begin{array}{lllll} z_0, & z_0^{(1)}, & z_0^{(2)}, & \ldots, & z_0^{(q-1)}, \\ z_1, & z_1^{(1)}, & z_1^{(2)}, & \ldots, & z_1^{(q-1)}, \\ \ldots & \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ z_{p-1} & z_{p-1}^{(1)}, & z_{p-1}^{(2)}, & \ldots, & z_{p-1}^{(q-1)}, \end{array}$$

de telle manière que si l'on adjoint à l'équation proposée une quelconque des racines d'un même groupe,

$$z_i, \; z_i^{(1)}, \; z_i^{(2)}, \; \ldots, \; z_i^{(q-1)},$$

le système conjugué Γ_i *propre à l'équation proposée sera*

([1]) Galois fait intervenir un groupe de permutations correspondant au système conjugué dont il est ici question, et il l'appelle le *groupe de l'équation.*

le même, quelle que soit la racine adjointe. En outre, les p systèmes conjugués

$$\Gamma,\ \Gamma_1,\ \Gamma_2,\ \ldots,\ \Gamma_{p-1},$$

qui deviennent propres à l'équation quand on adjoint respectivement une racine des groupes successifs, seront semblables entre eux, en sorte que chacun de ces systèmes pourra se déduire du premier, en exécutant une même substitution dans les cycles qui composent les diverses substitutions de celui-ci. Il est évident que chaque groupe se réduit à une seule racine si m est premier.

Désignons toujours par V la fonction résolvante et par

$$(3) \qquad F(V) = 0$$

l'équation irréductible de degré ν que nous avons nommée *équation résolvante;* soient aussi

$$V_0,\ V_1,\ V_2,\ \ldots,\ V_{\nu-1}$$

les ν racines de l'équation (3).

Si, après l'adjonction d'une racine z_0 de l'équation (2), l'équation (3) reste irréductible, il est clair que G demeurera le système conjugué propre à l'équation (1). Mais il n'en sera plus ainsi si l'équation (3) se réduit: c'est le cas que nous avons à examiner.

Soient $\lambda(V, z_0)$ l'un des facteurs irréductibles de $F(V)$ et μ le degré de ce facteur; on peut supposer que, dans le polynôme λ, le coefficient de la plus haute puissance de V soit l'unité et que les autres coefficients soient des fonctions entières de la racine z_0. Cela posé, z étant regardée comme une indéterminée, effectuons la division des polynômes $F(V)$, $\lambda(V, z)$ et désignons par $\Lambda(V, z)$, $\Theta(V, z)$ le quotient et le reste de cette division; on

aura

$$F(V) = \lambda(V, z)\Lambda(V, z) + \Theta(V, z),$$

et, d'après notre hypothèse, on a identiquement

$$\Theta(V, z_0) = 0;$$

car le polynôme $\Theta(V, z)$ est au plus du degré $\mu - 1$ en V, et la précédente équation est satisfaite par chacune des μ racines V de l'équation

$$\lambda(V, z_0) = 0.$$

Ainsi, dans le polynôme $\Theta(V, z)$, les coefficients des diverses puissances de V doivent s'annuler pour $z = z_0$; par conséquent, ces coefficients s'annuleront aussi si l'on y remplace z par une quelconque des racines de l'équation (2), puisque celle-ci est supposée irréductible.

D'après cela, si l'on représente par

$$z_0,\ z_1,\ z_2,\ \ldots,\ z_{m-1}$$

les m racines de l'équation (2), le polynôme F(V) sera divisible par chacune des fonctions

$$\lambda(V, z_0),\ \lambda(V, z_1),\ \ldots,\ \lambda(V, z_{m-1}).$$

Le produit de ces fonctions est une fonction entière de V dans laquelle les coefficients sont des fonctions symétriques des racines z; donc ce produit, que nous représenterons par $\Pi(V)$, est exprimable rationnellement par les quantités connues.

Les racines de l'équation

$$\Pi(V) = 0$$

appartiennent toutes à l'équation (3), et, puisque celle-ci est actuellement irréductible, le polynôme $\Pi(V)$ est divisible par F(V). Soit q l'exposant de la plus haute puis-

sance de $F(V)$ qui divise exactement $\Pi(V)$ et posons

$$\Pi(V) = [F(V)]^q \, \Pi_1(V),$$

il est évident que $\Pi_1(V)$ doit se réduire à une constante, ou, si l'on veut, à l'unité, puisque, dans nos polynômes, le coefficient du terme le plus élevé est égal à 1. En effet, si le contraire avait lieu, l'équation

$$\Pi_1(V) = 0$$

n'ayant que des racines appartenant à l'équation (3), $\Pi_1(V)$ serait divisible par $F(V)$, et l'exposant q ne satisferait pas à la condition qui lui a été imposée. Ainsi l'on a

$$\Pi(V) = [F(V)]^q$$

ou

$$(4) \qquad [F(V)]^q = \lambda(V, z_0)\lambda(V, z_1)\ldots\lambda(V, z_{m-1}).$$

D'après notre hypothèse, le polynôme $\lambda(V, z_0)$ est irréductible, c'est-à-dire qu'il n'admet aucun diviseur de degré inférieur au sien, dans lequel les coefficients seraient des fonctions rationnelles des quantités connues et de la racine adjointe de z_0. Je dis que le polynôme $\lambda(V, z_i)$ a lui-même la propriété de n'admettre aucun diviseur dans lequel les coefficients des puissances de V seraient des fonctions rationnelles des quantités connues et de la racine z_i. En effet, supposons qu'un tel diviseur existe et désignons-le par $\zeta(V, z_i)$; effectuons la division de $\lambda(V, z)$ par $\zeta(V, z)$, jusqu'à ce qu'on parvienne à un reste d'un degré inférieur à celui de $\zeta(V, z)$ relativement à V ; nommons $Q(V, z)$ et $R(V, z)$ le quotient et le reste de cette division. On aura

$$\lambda(V, z) = \zeta(V, z)Q(V, z) + R(V, z) ;$$

et, puisque $R(V, z)$ est nul pour $z = z_i$, on en conclura, par un raisonnement dont nous avons fait usage plus

haut, que le même reste est nul, quelle que soit celle des racines de l'équation (2) que l'on substitue à z; on aura en particulier

$$R(V, z_0) = 0,$$

ce qui exprime que $\lambda(V, z_0)$ admet le diviseur $\zeta(V, z_0)$. Cette conclusion est contraire à l'hypothèse, et, par conséquent, notre assertion se trouve justifiée.

Les racines de l'équation (3) sont toutes exprimables en fonction rationnelle de l'une quelconque d'entre elles. Cela étant rappelé, considérons les deux équations

$$(5) \qquad \lambda(V, z_i) = 0, \quad \lambda(V, z_j) = 0,$$

et désignons par V_α et $\theta(V_\alpha)$ deux racines de la première, θ étant une fonction rationnelle. Je dis que, si V_β est une racine de la deuxième équation (5), $\theta(V_\beta)$ sera également racine de la même équation. En effet, on a

$$\lambda(V_\alpha, z_i) = 0, \quad \lambda[\theta(V_\alpha), z_i] = 0;$$

en d'autres termes, l'équation

$$\lambda[\theta(V), z_i] = 0$$

est satisfaite quand on remplace V par la racine V_α de l'équation

$$\lambda(V, z_i) = 0;$$

elle admettra donc toutes les racines de cette dernière, car celle-ci n'a aucun diviseur dont les coefficients sont fonctions rationnelles de z_i, ainsi que nous venons de le démontrer. Si l'on suppose, comme cela est permis, que $\theta(V)$ soit une fonction entière, on peut dire que le polynôme $\lambda[\theta(V), z_i]$ est divisible par $\lambda(V, z_i)$, ou que le reste de la division du polynôme

$$\lambda[\theta(V), z]$$

par $\lambda(V, z)$ est identiquement nul pour $z = z_i$. Alors, par le raisonnement déjà employé deux fois dans cette démonstration, on conclura que le même reste est nul aussi pour $z = z_j$, c'est-à-dire que $\lambda[\theta(V), z_j]$ est divisible par $\lambda(V, z_j)$; par suite l'égalité

$$\lambda(V_6, z_j) = 0$$

entraînera

$$\lambda[\theta(V_6), z_j] = 0$$

ce qui exprime que $\theta(V_6)$ est racine de la deuxième équation (5). Nous concluons de là que, si les équations (5) ont une racine commune, elles ont toutes leurs racines communes.

Cette analyse établit que, dans le second membre de la formule (4), chacun des facteurs inégaux se trouve répété q fois. En employant deux indices pour représenter les m racines z, on aura

$$\begin{array}{l}
\lambda(V, z_0) = \lambda(V, z_0^{(1)}) = \lambda(V, z_0^{(2)}) = \ldots = \lambda(V, z_0^{(q-1)}),\\
\lambda(V, z_1) = \lambda(V, z_1^{(1)}) = \lambda(V, z_1^{(2)}) = \ldots = \lambda(V, z_1^{(q-1)}),\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\lambda(V, z_{p-1}) = \lambda(V, z_{p-1}^{(1)}) = \lambda(V, z_{p-1}^{(2)}) = \ldots = \lambda(V, z_{p-1}^{(q-1)}),
\end{array}$$

et, en extrayant la racine $q^{\text{ième}}$ des deux membres de la formule (4), on aura

$$(6) \qquad F(V) = \lambda(V, z_0)\lambda(V, z_1)\ldots\lambda(V, z_{p-1}),$$

car, dans les polynômes F et λ, on peut supposer les coefficients des premiers termes réduits à l'unité.

Ainsi les m racines z se partagent en p groupes contenant chacun q racines; en outre, quelle que soit celle des racines d'un même groupe que l'on adjoigne à l'équation proposée, cette adjonction aura le même effet, savoir de substituer à l'équation résolvante primitive

le même diviseur de cette équation. Et, par conséquent, le système conjugué propre à l'équation proposée se trouvera lui-même réduit à un nouveau système dont l'ordre sera un diviseur de l'ordre du système primitif.

Il nous reste à comparer entre eux les divers systèmes conjugués Γ, $\Gamma_1, \ldots, \Gamma_{p-1}$ qui deviennent ainsi propres à l'équation proposée, quand on adjoint respectivement à celle-ci une racine des groupes correspondants que nous avons distingués.

Les racines de l'équation

$$\lambda(V, z_0) = 0$$

étant des fonctions rationnelles de l'une d'entre elles, représentons-les par

$$V_0, \ \theta_1(V_0), \ \theta_2(V_0), \ \ldots, \ \theta_{\mu-1}(V_0)$$

soit aussi $V_0^{(i)}$ une racine de l'équation

$$\lambda(V, z_i) = 0,$$

les quantités

$$V_0^{(i)}, \ \theta_1(V_0^{(i)}), \ \theta_2(V_0^{(i)}), \ \ldots, \ \theta_{\mu-1}(V_0^{(i)})$$

seront racines de la même équation, comme nous l'avons dit plus haut ; j'ajoute qu'elles sont distinctes, en sorte qu'aucune racine ne se trouve omise. En effet, V_0 et $V_0^{(i)}$ étant racines de l'équation (3) qui est *actuellement* irréductible, si l'on avait

$$\theta_\alpha(V_0^{(i)}) = \theta_6(V_0^{(i)})$$

il en résulterait

$$\theta_\alpha(V_0) = \theta_6(V_0),$$

ce qui est contraire à notre hypothèse.

Maintenant, V désignant l'une quelconque des racines de la résolvante (3), représentons par le symbole

$$[V]$$

la permutation

$$\psi_0(V),\ \psi_1(V),\ \psi_2(V),\ \ldots,\ \psi_{n-1}(V)$$

des racines de la proposée, et posons

$$(7)\qquad [\theta_k(V_0)] = S_k[V_0],\quad [\theta_k(V_0^{(i)})] = S_k^{(i)}[(V_0^{(i)})];$$

les substitutions du système Γ seront

$$1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1},$$

et celles du système Γ_i seront

$$1,\ S_1^{(i)},\ S_2^{(i)},\ \ldots,\ S_{\mu-1}^{(i)}.$$

Représentons enfin par T_i la substitution par laquelle on passe de la permutation $[V_0]$ à la permutation $[V_0^{(i)}]$; on aura, non-seulement

$$(8)\qquad [V_0^{(i)}] = T_i[V_0],$$

mais encore, quel que soit k,

$$[\theta_k(V_0^{(i)})] = T_i[\theta_k(V_0)],$$

ou, à cause de la première des formules (7),

$$(9)\qquad [\theta_k(V_0^{(i)})] = T_iS_k[V_0];$$

enfin la formule (8) réduit la seconde formule (7) à

$$(10)\qquad [\theta_k(V_0^{(i)})] = S_k^{(i)}T_i[V_0],$$

et la comparaison des formules (9) et (10) donne

$$(11)\qquad S_k^{(i)}T_i = T_iS_k;$$

d'où

$$(12) \qquad S_k^{(i)} = T_i S_k T_i^{-1}.$$

Les formules (8) et (9) expriment que le système conjugué G est représenté par

$$(13) \quad \left\{ \begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ T_1, & T_1 S_1, & T_1 S_2, & \ldots, & T_1 S_{\mu-1}, \\ T_2, & T_2, S_1 & T_2 S_2, & \ldots, & T_2 S_{\mu-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots, \\ T_{p-1}, & T_{p-1} S_1, & T_{p-1} S_2, & \ldots, & T_{p-1} S_{\mu-1}, \end{array} \right.$$

et la formule (12) exprime que les systèmes Γ, $\Gamma_1, \ldots,$ Γ_{p-1} sont

$$(14) \quad \left\{ \begin{array}{lllll} \Gamma = 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ \Gamma_1 = 1, & T_1 S_1 T_1^{-1}, & T_1 S_2 T_1^{-1}, & \ldots, & T_1 S_{\mu-1} T_1^{-1}, \\ \Gamma_2 = 1, & T_2 S_1 T_2^{-1}, & T_2 S_2 T_2^{-1}, & \ldots, & T_2 S_{\mu-1} T_2^{-1}, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \Gamma_{p-1} = 1, & T_{p-1} S_1 T_{p-1}^{-1}, & \ldots, & & T_{p-1} S_{\mu-1} T_{p-1}^{-1}. \end{array} \right.$$

Ces systèmes sont, comme on le voit, semblables, en sorte que chacun d'eux peut se déduire du premier Γ en exécutant dans les cycles de chacune des substitutions de celui-ci une même substitution T, ce qui achève la démonstration du théorème énoncé.

581. Théorème IV. — *Si le système* G *propre à l'équation* $f(x) = 0$ *se réduit à un système* Γ *d'ordre inférieur, par l'adjonction d'une racine de l'équation auxiliaire irréductible* $\varphi(z) = 0$; *si, en outre, les racines de cette équation auxiliaire sont exprimables rationnellement en fonction de l'une d'entre elles et des quantités connues, le système* Γ *ne changera pas quand*

on exécutera dans les cycles de toutes ses substitutions une substitution quelconque du système G.

En effet, soient

$$z_0 \quad \text{et} \quad z_i = \theta z_0$$

deux racines de l'équation auxiliaire : θ désigne ici une fonction rationnelle; l'équation $\varphi(z) = 0$ étant supposée irréductible, elle admettra toutes les racines

$$z_0, \ \theta z_0, \ \theta^2 z_0, \ \ldots, \ \theta^{k-1} z_0;$$

l'un des termes de cette suite se réduira à z_0, et si l'on suppose

$$\theta^k z_0 = z_0 \quad \text{ou} \quad \theta^{k-1}\theta z_0 = z_0,$$

il en résultera

$$z_0 = \theta^{k-1} z_i;$$

par conséquent les racines z_0 et z_i sont exprimables rationnellement l'une par l'autre.

Il s'ensuit que les quantités connues sont les mêmes après l'adjonction de z_0 ou après celle de z_i; le système Γ_i propre à l'équation $f(x) = 0$, après l'adjonction de z_i, est donc le même que le système Γ qui est propre à l'équation après l'adjonction de z_0. Et, comme les systèmes Γ, Γ_i peuvent être représentés par

$$\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ 1, & T_i S_1 T_i^{-1}, & T_i S_2 T_i^{-1}, & \ldots, & T_i S_{\mu-1} T_i^{-1}, \end{array}$$

on voit que le système Γ ne changera pas si l'on multiplie ces substitutions à droite par T_i et à gauche par T_i^{-1}, opération qui revient à exécuter la substitution T_i dans les cycles des substitutions de Γ.

Enfin, toute substitution de G est la forme

$$U = T_k S_h,$$

ce qui donne

$$U^{-1} = S_h^{-1} T_k^{-1},$$

d'où

$$US'U^{-1} = T_k S_h S_i S_h^{-1} T_k^{-1}.$$

Par conséquent, si l'on veut exécuter la substitution U dans les cycles des substitutions de Γ, il suffira de faire, dans ces cycles, d'abord la substitution S_h, puis la substitution T_k; il est évident que la première opération ne changera pas Γ, puisque S_h fait partie de ce système : d'ailleurs nous venons de prouver que la deuxième opération ne produit elle-même aucun changement sur Γ; donc ce système reste invariable quand on exécute la substitution U dans les cycles de toutes ses substitutions.

Corollaire. — *Si l'équation auxiliaire est de la forme $z^p = A$, et que les racines $p^{\text{ièmes}}$ de l'unité se trouvent au nombre des quantités précédemment adjointes, on se trouvera dans les conditions du précédent théorème.*

582. Théorème V. — *Si le système conjugué G_1, propre à l'équation $f(x) = 0$, se réduit à un système Γ d'ordre inférieur, quand on adjoint à l'équation* toutes *les racines d'une équation auxiliaire irréductible $\varphi(z) = 0$, de degré m, le système Γ ne changera pas quand on exécutera, dans les cycles de toutes ses substitutions, une quelconque des substitutions du système* G (¹).

En effet, soit Z une fonction rationnelle des m racines

(1) $$z_0, z_1, z_2, \ldots, z_{m-1}$$

(¹) Ce théorème ne diffère pas au fond de la proposition III du Mémoire de Galois. Sous ce titre de proposition III, Galois avait d'abord inscrit l'énoncé du corollaire de notre théorème IV, avec une démonstration, mais il a effacé le tout pour y substituer l'énoncé qu'il a adopté définitivement.

de l'équation auxiliaire, telle que les

$$M = 1.2.3\ldots m$$

fonctions qu'on en déduit par les substitutions aient des valeurs différentes ; soient en outre

$$\mathfrak{F}(Z) = 0$$

l'équation du degré M qui a pour racines les M valeurs de Z, F(Z) un diviseur irréductible de $\mathfrak{F}(Z)$, et

$$(2) \qquad Z_0,\ Z_1,\ Z_2,\ \ldots,\ Z_{\mu-1}$$

les μ racines de l'équation

$$(3) \qquad F(Z) = 0.$$

Les quantités (2) sont des fonctions rationnelles des quantités (1), et réciproquement celles-ci peuvent s'exprimer en fonction rationnelle des quantités (2) (n° 502) : donc l'adjonction des unes entraîne l'adjonction des autres. Par conséquent, d'après notre hypothèse, le système G, propre à l'équation proposée, doit se réduire, par l'adjonction des racines de l'équation (3). Mais ces racines peuvent s'exprimer rationnellement en fonction de l'une quelconque d'entre elles ; donc l'adjonction d'une seule racine équivaut à l'adjonction de toutes, et l'on se trouve alors dans les conditions du théorème IV.

583. Théorème VI. — *Soient* G *le système conjugué propre à l'équation*

$$(1) \qquad f(x) = 0$$

et

$$(2) \qquad z_0 = \mathfrak{F}(x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1})$$

une fonction rationnelle des n racines $x_0, x_1, x_2, \ldots, x_{n-1}$,

dont la valeur numérique ne soit pas actuellement connue. Si l'on adjoint cette valeur numérique à l'équation proposée, le système Γ *propre à l'équation, après l'adjonction, sera formé par celles des substitutions de* G *qui n'altèrent pas la valeur numérique de la fonction* $\mathfrak{F}$.

Les conditions de ce théorème se ramènent immédiatement à celles du théorème III. Exécutons toutes les substitutions des racines x dans l'expression

$$z - \mathfrak{F}(x_0, x_1, x_2, \ldots, x_{n-1}),$$

et formons le produit $\Phi(z)$ de tous les résultats obtenus. Les coefficients du polynôme $\Phi(z)$ seront des fonctions symétriques des racines x, et par conséquent ils seront rationnellement connus; décomposons ce polynôme en ses facteurs irréductibles, et désignons par $\varphi(z)$ l'un de ces facteurs qui s'annulent pour $z = z_0$. Nous nous trouvons placés alors dans le cas où l'on adjoint à l'équation proposée la racine z_0 de l'équation irréductible

$$(3) \qquad \varphi(z) = 0.$$

Soient, comme dans le théorème III,

$$V_0, V_1, \ldots, V_{\nu-1}$$

les ν racines de la résolvante

$$(4) \qquad F(V) = 0,$$

qui est actuellement irréductible. Les racines x étant exprimables rationnellement par l'une quelconque des racines V, posons aussi, comme précédemment,

$$x_0 = \psi_0(V_0), \quad x_1 = \psi_1(V_0), \quad \ldots, \quad x_{n-1} = \psi_{n-1}(V_0);$$

la formule (2) deviendra

$$z_0 = \mathfrak{F}[\psi_0(V_0), \psi_1(V_0), \ldots, \psi_{n-1}(V_0)] = \Psi(V_0),$$

et l'on peut faire en sorte (n° 182) que Ψ soit une fonction entière d'un degré inférieur à ν. Alors l'équation

(5) $$\Psi(V) - z_0 = 0$$

admet la racine V_0 de l'équation (4). Soient

(6) $$V_0,\ V_1,\ \ldots,\ V_{\mu-1}$$

les μ racines communes aux équations (4) et (5), et posons

$$\lambda(V, z_0) = (V - V_0)(V - V_1)\ldots(V - V_{\mu-1});$$

les coefficients de l'équation

(7) $$\lambda(V, z_0) = 0$$

sont rationnels après l'adjonction de z_0 : je dis que cette équation est irréductible. En effet, si le contraire a lieu, soit $\varpi(V, z_0)$ le diviseur irréductible de $\lambda(V, z_0)$ qui s'annule pour $V = V_0$; on aura (théorème III)

$$F(V) = \varpi(V, z_0)\,\varpi(V, z_1)\ldots\varpi(V, z_{p-1}),$$

$z_1, z_2, \ldots, z_{p-1}$ étant des racines de l'équation (2) distinctes de z_0 ; l'équation

$$\varpi(V, z_0) = 0$$

n'admettra qu'une partie des racines (6), et l'une de ces racines, V_1 par exemple, devra satisfaire à une équation telle que

(8) $$\varpi(V, z_1) = 0.$$

Effectuons la division de $\Psi(V) - z$ par $\varpi(V, z)$ jusqu'à ce que nous parvenions à un reste de degré inférieur au diviseur; désignons par $\Theta(V, z)$ ce reste, et par $\Pi(V, z)$ le quotient de la division; on aura

$$\Psi(V) - z = \varpi(V, z)\,\Pi(V, z) + \Theta(V, z);$$

par hypothèse, $\Psi(V) - z_0$ est divisible par $\lambda(V, z_0)$; ce polynôme l'est donc aussi par $\varpi(V, z_0)$, et en conséquence, le reste $\Theta(V, z)$ de la précédente division, se réduit identiquement à zéro pour $z = z_0$. Alors, par un raisonnement déjà employé, nous concluons que le même reste est nul pour $z = z_1$, et l'on a

$$\Psi(V) - z_1 = \varpi(V, z_1)\Pi(V, z_1).$$

Maintenant nous avons supposé que V_1 est une racine de l'équation (8) ; on a donc

$$\Psi(V_1) = z_1,$$

ce qui est impossible, puisque V_1 est racine de l'équation (5), et que z_1 est différente de z_0.

Nous concluons de là que l'équation (7) est irréductible, en sorte qu'elle devient l'équation résolvante, après l'adjonction de z_0. Le système conjugué propre à l'équation proposée se compose alors des μ substitutions qu'on exécute en remplaçant V_0 par chacune des quantités (6) dans la permutation des racines

$$\psi_0(V_0),\ \psi_1(V_0),\ \ldots,\ \psi_{n-1}(V_0).$$

D'ailleurs les quantités (6) sont celles des racines de l'équation (5) qui appartiennent à la résolvante primitive; donc les substitutions dont nous venons de parler sont celles par lesquelles la valeur numérique z_0 de la fonction $\mathcal{F}(x_0, x_1, \ldots, x_{n-1})$ reste invariable.

584. Théorème VII. — *Le nombre p étant premier, soit $\nu = \mu p$ l'ordre du système conjugué* G *propre à une équation $f(x) = 0$. Si l'on peut former avec μ substitutions de* G *un système conjugué* Γ *qui reste invariable quand on exécute dans les cycles de toutes ses substitutions les diverses substitutions de* G, *il suffira d'extraire la racine $p^{\text{ième}}$ d'une certaine quantité rationnelle, et*

d'adjoindre cette racine $p^{\text{ième}}$ à l'équation, pour que Γ *devienne le système propre à cette équation. On suppose que les racines $p^{\text{ièmes}}$ de l'unité font partie des quantités précédemment adjointes.*

Soient

$$(1) \qquad 1,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1}$$

les substitutions du système Γ, et T une substitution de G qui n'appartienne pas à Γ; on aura, par hypothèse, quel que soit i,

$$(2) \qquad TS_iT^{-1} = S_j,$$

j étant un indice convenablement choisi. Si le système des puissances de T,

$$(3) \qquad 1,\ T,\ T^2,\ \ldots,\ T^{t-1},$$

d'ordre t, a quelques substitutions communes autres que l'unité avec le système (1), soit T^α la plus petite puissance de T contenue dans ce système. En multipliant les substitutions (1) par les substitutions

$$1,\ T,\ T^2,\ \ldots,\ T^{\alpha-1},$$

on obtiendra les $\mu\alpha$ produits

$$(4) \qquad \left\{\begin{array}{lllll} 1, & S_1, & S_2, & \ldots, & S_{\mu-1}, \\ T, & TS_1, & TS_2, & \ldots, & TS_{\mu-1}, \\ \ldots & \ldots & \ldots\ldots\ldots & & \ldots\ldots \\ T^{\alpha-1}, & T^{\alpha-1}S_1, & \ldots\ldots\ldots, & & T^{\alpha-1}S_{\mu-1}, \end{array}\right.$$

qui seront distincts; car, si l'on avait

$$T^iS_g = T_{i+j}S_h,$$

on en conclurait

$$T_j = S_g S_h^{-1},$$

ce qui ne peut pas avoir lieu, puisque la substitution $S_g S_h^{-1}$ fait partie du système (1), tandis qu'il n'en est pas ainsi à l'égard de T^j à cause de $j < \alpha$. Ensuite le produit de deux quelconques des substitutions (4) peut être ramené par la formule (2) à la forme

$$T^{g\alpha+h} S_k \text{ ou } T^h S_k,$$

h étant $< \alpha$, et ce produit est l'une des substitutions (4). Ces substitutions forment ainsi un système conjugué d'ordre $\mu\alpha$; elles sont d'ailleurs contenues dans le système G dont l'ordre est μp: donc μp est divisible par $\mu\alpha$ et p par α; il s'ensuit que α est égal à 1 ou à p, puisque p est un nombre premier. Si $\alpha = 1$, la substitution T appartient à Γ, ce qui est contraire à l'hypothèse. Ainsi $\alpha = p$; mais alors le système (4) contient μp substitutions, et, par conséquent, il n'est autre que le système G. Les puissances de T contenues dans Γ sont donc

$$1,\ T^p,\ T^{2p},\ \ldots,\ T^{(k-1)p},$$

et l'on a

$$T^{kp} = 1;$$

on a d'ailleurs évidemment

$$(k-1)p = \text{ou} < t-1, \quad kp = qt,$$

q étant un entier, ce qui exige que $q = 1$, en sorte que l'ordre de la substitution T est nécessairement égal à p ou à un multiple de p.

Cela posé, soit Θ une fonction rationnelle des n racines $x_0, x_1, x_2, \ldots, x_{n-1}$ de l'équation $f(x) = 0$, telle que les $1.2.3\ldots n$ fonctions qu'on en déduit par les substitutions aient des valeurs numériques inégales. Exécutons sur cette fonction les μ substitutions (1) de Γ et désignons par

(3) $$\Theta_0,\ \Theta_1,\ \Theta_2,\ \ldots,\ \Theta_{\mu-1}$$

les résultats obtenus. Prenons enfin une fonction rationnelle et symétrique θ des μ quantités (3); on pourra faire, par exemple,

(4) $$\theta = (\Theta - \Theta_0)(\Theta - \Theta_1)\ldots(\Theta - \Theta_{\mu-1}),$$

Θ désignant ici une indéterminée.

La fonction θ est invariable par les substitutions de Γ, mais elle varie par toute autre substitution; exécutons sur cette fonction les puissances de la substitution T, savoir :

$$1,\ T,\ T^2,\ \ldots,\ T^{p-1},$$

et désignons par θ_i le résultat obtenu par la substitution T^i. Représentons aussi par α une racine de l'équation

$$\frac{x^p - 1}{x - 1} = 0,$$

et posons

$$(\theta_0 + \alpha\theta_1 + \alpha^2\theta_2 + \ldots + \alpha^{p-1}\theta_{p-1})^p = \Omega;$$

la fonction Ω est évidemment invariable par la substitution T qui a pour effet de déplacer circulairement les quantités

$$\theta_0,\ \theta_1,\ \theta_2,\ \ldots,\ \theta_{p-1};$$

elle ne varie pas non plus par les substitutions de Γ, car on a

$$\theta_i = T^i\theta_0,$$

et, en exécutant une substitution S,

$$S_j\theta_i = S_j T^i\theta_0 = T^i S_k\theta_0 = T^i\theta_0 = \theta_i.$$

On peut conclure de là que la fonction Ω est invariable par toutes les substitutions du système G, qui est actuellement propre à l'équation proposée. Il s'ensuit que la valeur de Ω est actuellement connue; si donc on adjoint à l'équation le radical

$$\sqrt[p]{\Omega},$$

la fonction

$$\theta_0 + \alpha\theta_1 + \alpha^2\theta_2 + \ldots + \alpha^{p-1}\theta_{p-1} = \sqrt[p]{\Omega}$$

sera connue.

Les seules substitutions qui laissent cette fonction invariable sont celles de Γ, et, par conséquent, d'après le théorème VI, Γ devient, par l'adjonction de $\sqrt[p]{\Omega}$, le système conjugué propre à l'équation.

585. Les propositions que nous venons d'établir permettent d'aborder la solution de ce problème :

Dans quel cas une équation est-elle résoluble par radicaux ?

A cet effet, Galois observe que, dès qu'une équation est résolue, une fonction quelconque de ses racines est connue, même lorsqu'elle n'est invariable par aucune substitution. En conséquence, le système conjugué propre à l'équation ne contient plus alors que la seule substitution identique, celle qui est égale à l'unité.

La solution du problème qui a pour objet la résolution d'une équation doit donc consister dans l'abaissement successif de l'ordre du système conjugué propre à l'équation.

« Suivons, dit Galois, la marche des opérations pos-
» sibles dans cette solution, en considérant comme opé-
» rations distinctes l'extraction de chaque racine de de-
» gré premier.

» Adjoignons à l'équation le premier radical extrait
» dans la solution. Il pourra arriver deux cas : ou bien,
» par l'adjonction de ce radical, *l'ordre du système con-*
» *jugué propre à l'équation* sera diminué (1); ou bien,

(1) J'indique par des italiques les légers changements que nécessite ici l'emploi exclusif des systèmes de substitutions que nous avons adoptés au lieu des groupes de permutations dont Galois fait usage.

» cette extraction de racine n'étant qu'une simple pré-
» paration, le *système propre à l'équation* restera le
» même.

» Toujours sera-t-il qu'après un certain nombre *fini*
» d'extractions de racines, *l'ordre du système propre à*
» *l'équation* devra se trouver diminué, sans quoi l'équa-
» tion ne serait pas soluble.

» Si, arrivé à ce point, il y avait plusieurs manières
» de diminuer l'ordre du *système propre à l'équation*
» proposée par une simple extraction de racine, il fau-
» drait, pour ce que nous allons dire, considérer seule-
» ment un radical du degré le moins haut possible parmi
» tous les simples radicaux, qui sont tels, que la connais-
» sance de chacun d'eux diminue l'*ordre du système*
» *propre à l'équation*.

» Soit donc p le nombre premier qui représente ce
» degré minimum, en sorte que par une extraction de
» racine de degré p on diminue l'*ordre du système propre*
» *à l'équation*.

» Nous pouvons toujours supposer, du moins pour ce
» qui est relatif au *système propre à l'équation*, que,
» parmi les quantités adjointes précédemment à l'équa-
» tion, se trouve une racine $p^{\text{ième}}$ de l'unité ; car, comme
» cette expression s'obtient par des extractions de racines
» de degrés inférieurs à p, sa connaissance n'altérera en
» rien le *système propre à l'équation*. »

On voit ici toute l'importance des théorèmes III et IV. Dans l'hypothèse admise, le système conjugué propre à l'équation qui est actuellement G se réduit à un système Γ d'ordre inférieur; il en résulte, d'après les théorèmes III et IV (corollaire), que l'ordre de Γ est un diviseur de l'ordre G, et que ce système reste invariable quand on exécute dans les cycles de toutes ses substitutions l'une

quelconque des substitutions de G. Et réciproquement, d'après la proposition VII, G étant le système d'ordre $\nu = \mu p$ actuellement propre à l'équation, si l'on peut trouver un système Γ d'ordre μ qui soit contenu dans G, et qui reste invariable quand on exécute les substitutions de G dans les cycles de toutes ses substitutions, Γ deviendra, par l'extraction d'une racine $p^{\text{ième}}$ et par l'adjonction de cette racine, le système propre à l'équation.

Ainsi ces propositions découvertes par Galois, et dont nous avons donné des démonstrations complètes et rigoureuses, indiquent la condition nécessaire et suffisante pour l'abaissement de l'ordre du système conjugué propre à l'équation.

Cet ordre ayant été abaissé une première fois par l'adjonction d'un radical, on peut raisonner sur le nouveau système conjugué comme sur le précédent, et il faudra qu'il se réduise aussi de la même manière, et ainsi de suite, jusqu'à ce qu'on arrive à un système qui ne contienne plus que la seule substitution égale à l'unité.

586. Il est aisé d'observer cette marche, comme l'a remarqué Galois, dans la résolution connue de l'équation générale du quatrième degré.

Soient

$$a,\ b,\ c,\ d$$

les racines. Le système conjugué G propre à l'équation est ici le système des $1.2.3.4 = 24$ substitutions des quatre racines, et l'on obtient (n° 443), en faisant le produit des quatre systèmes,

$$\begin{array}{l} 1,\ (a,b)(c,d), \\ 1,\ (a,c)(b,d), \\ 1,\ (b,c,d),\ (b,d,c), \\ 1,\ (b,c). \end{array}$$

L'équation dont il s'agit se résout au moyen d'une équation du troisième degré, laquelle exige l'extraction d'une racine carrée. Dans la suite naturelle des idées, c'est par cette racine qu'il faut commencer. En adjoignant cette racine carrée à l'équation proposée, on réduit à 12 (théorème VII) l'ordre du système conjugué propre à l'équation, lequel devient alors égal au produit des trois

$$1,\ (a, b)(c, d),$$
$$1,\ (a, c)(b, d),$$
$$1,\ (b, c, d),\ (b, d, c).$$

Maintenant, par l'extraction d'une racine cubique, on réduira à 4 l'ordre du système propre à l'équation; ce système est le produit des deux

$$1,\ (a, b)(c, d),$$
$$1,\ (a, c)(b, d).$$

L'extraction d'une racine carrée réduira à 2 l'ordre du système qui deviendra ainsi

$$1,\ (a, b)(c, d);$$

enfin, par une dernière extraction de racine carrée, le système propre à l'équation se réduit à l'unité; alors l'équation est résolue.

Suite des recherches de Galois. — Applications aux équations irréductibles de degré premier.

587. Les applications de la théorie que nous venons d'exposer offrent encore bien des difficultés (¹). Nous

(¹) M. C. Jordan a présenté à l'Académie des Sciences des recherches nouvelles sur ce sujet.

nous bornerons à celle que Galois en a faite aux équations irréductibles dont le degré est un nombre premier.

LEMME. — *Une équation irréductible de degré premier ne peut devenir réductible par l'adjonction d'un radical dont l'indice serait autre que le degré même de l'équation.*

En effet, supposons que l'équation irréductible

$$(1) \qquad f(x) = 0,$$

de degré premier n, devienne réductible par l'adjonction d'un radical. Comme l'extraction d'une racine de degré composé se ramène à des extractions successives de racines de degrés premiers, on peut supposer que l'indice du radical dont il s'agit est un nombre premier. Seulement, si la quantité soumise à ce radical ne fait pas partie des quantités actuellement connues, on devra la regarder comme adjointe à l'équation.

Cela posé, soit m le plus petit nombre premier tel, que l'équation (1) devienne réductible par l'adjonction d'une racine d'une équation de la forme

$$(2) \qquad z^m = A,$$

A étant une quantité connue ou une quantité dont l'adjonction laisse l'équation (1) irréductible. Les racines de l'équation

$$(3) \qquad z^m = 1$$

peuvent être regardées comme faisant partie des quantités connues, en ce sens que ces racines s'obtiennent par des extractions de racines de degrés inférieurs à m, et que, d'après notre hypothèse, leur connaissance ne suffit pas pour effectuer la réduction de l'équation.

Soient r une racine de l'équation (2) et α une racine

primitive de l'équation (3); les racines de l'équation (2) seront

$$r,\ \alpha r,\ \alpha^2 r,\ \ldots,\ \alpha^{m-1} r.$$

Maintenant, si l'adjonction de r réduit l'équation (1), soit $\varphi(x, r)$ le diviseur irréductible de $f(x)$ qui a le moindre degré; le polynôme $f(x)$ sera divisible par chacune des fonctions

$$\varphi(x, r),\ \varphi(x, \alpha r),\ \ldots,\ \varphi(x, \alpha^{m-1} r).$$

Le produit de ces diviseurs est une fonction symétrique des racines de l'équation (2), et, par suite, il est exprimable rationnellement par les quantités connues; d'ailleurs ce produit ne peut s'annuler que pour les valeurs de x qui satisfont à l'équation (1); donc, puisque cette équation est irréductible, le produit dont il s'agit est nécessairement une puissance de $f(x)$, et l'on a

$$(4)\qquad [f(x)]^q = \varphi(x, r)\varphi(x, \alpha r)\ldots\varphi(x, \alpha^{m-1} r).$$

Si les deux équations

$$\varphi(x, \alpha^i r) = 0,\quad \varphi(x, \alpha^j r) = 0$$

ont une racine commune, elles ont toutes leurs racines communes; car, si le contraire avait lieu, les premiers membres de ces équations auraient un diviseur commun $\psi(x, r)$ qui serait rationnel relativement aux quantités connues, et $\varphi(x, r)$ ne serait pas le diviseur de $f(x)$ du degré minimum.

Alors, si l'on extrait la racine $q^{\text{ième}}$ des deux membres de la formule (4), on aura un résultat de la forme

$$(5)\qquad f(x) = \varphi(x, r)\varphi(x, \alpha r)\varphi(x, \beta r)\ldots\varphi(x, \varepsilon r),$$

$\alpha, \beta, \ldots, \varepsilon$ désignant des racines de l'équation (3). Mais, le degré de $f(x)$ étant un nombre premier, la formule (5)

ne peut avoir lieu que si les polynômes φ sont du premier degré, et la formule (4) montre que m est divisible par n; d'ailleurs m est premier : donc on a $m = n$.

Corollaire. — *Une équation irréductible de degré premier ne peut devenir réductible, à moins que le système conjugué qui lui est propre ne se réduise à la seule substitution égale à l'unité.*

En effet, d'après le lemme précédent, si l'équation proposée se réduit, son premier membre se décompose en facteurs linéaires, et, par suite, elle se trouve résolue.

588. Il nous reste à faire connaître les théorèmes par lesquels Galois a exprimé la condition de résolubilité des équations de degré premier.

Théorème I. — *Si une équation irréductible $f(x) = 0$, d'un degré premier n, est résoluble par radicaux, ses n racines pourront être représentées par x_z* [l'indice z, pris suivant le module n, devant être réduit à l'un des nombres $0, 1, 2, \ldots, (n-1)$], *de telle manière que le système conjugué actuellement propre à l'équation ne renferme que des substitutions linéaires et entières, c'est-à-dire des substitutions de la forme $\begin{pmatrix} az+b \\ z \end{pmatrix}$, a et b étant des constantes.*

En effet, l'adjonction successive de quantités radicales réduira, par hypothèse, à l'unité le système conjugué propre à l'équation, et, d'après le lemme précédent, cette équation restera irréductible jusqu'à la dernière adjonction. Celle-ci, qui est celle d'un radical d'indice n, opère non-seulement la réduction, mais encore la résolution de l'équation (n° 587), et, d'après le théorème du n° 580, elle divise par n l'ordre du système conjugué propre à l'équation.

Donc, immédiatement avant d'être réduit à l'unité, l'ordre du système propre à l'équation sera égal à n. Mais, quand l'ordre d'un système conjugué, relatif à un nombre premier n de lettres, est égal à n, le système se compose des puissances d'une substitution circulaire d'ordre n (n° 426, corollaire III); donc l'avant-dernier système propre à l'équation sera formé par les puissances d'une substitution qui sera représentée par

$$\begin{pmatrix} z+1 \\ z \end{pmatrix},$$

si les n indices ont été convenablement distribués entre les n racines. En d'autres termes, le système dont il s'agit se composera des n substitutions linéaires de la forme

$$\begin{pmatrix} z+b \\ z \end{pmatrix},$$

où l'on doit donner à b n valeurs congrues aux nombres

$$0,\ 1,\ 2,\ \ldots,\ (n-1)$$

suivant le module n, les indices étant pris, comme nous l'avons dit, suivant le même module.

Cela posé, je dis qu'en remontant de cet avant-dernier système jusqu'à celui qui est *actuellement* propre à l'équation, on ne rencontrera dans chaque système que des substitutions linéaires et entières de la forme

$$\begin{pmatrix} az+b \\ z \end{pmatrix}.$$

Cette proposition étant établie à l'égard de l'avant-dernier système, il nous suffit de démontrer que, si elle a lieu pour un système quelconque Γ, elle subsiste pour le système G qui précède immédiatement Γ dans l'ordre des réductions. A cet effet, remarquons que, si Γ n'est pas l'avant-

dernier système, il renferme néanmoins les substitutions de celui-ci ; soit S_i l'une d'elles, on aura

$$S_i = \begin{pmatrix} z + \beta \\ z \end{pmatrix},$$

β étant l'un des nombres 1, 2, 3, ..., $(n-1)$. Maintenant, si l'on désigne par T l'une quelconque des substitutions de G, on aura, quel que soit i, par le théorème du n° 581,

$$TS_iT_{-1} = S_j, \quad \text{ou} \quad TS_i = S_jT,$$

S_j étant une substitution de Γ : cette égalité exprime que S_j est une substitution semblable à S_i ; en conséquence, cette substitution est circulaire. Or, d'après notre hypothèse, le système Γ ne renferme que des substitutions linéaires et entières ; il s'ensuit que ce système ne peut avoir deux substitutions circulaires S_i et S_j d'ordre n qui ne seraient pas puissances l'une de l'autre, car autrement il contiendrait les n^2 produits de la forme $S_i^\alpha S_j^\beta$ qui seraient tous distincts, et cela est impossible, puisque le nombre total des substitutions linéaires est seulement $n(n-1)$. Ainsi S_j est une puissance de S_i, et l'on a

$$S_j = \begin{pmatrix} z + a \\ z \end{pmatrix}.$$

Posons

$$T = \begin{pmatrix} F(z) \\ z \end{pmatrix},$$

on aura

$$TS_i = \begin{pmatrix} F(z+\beta) \\ z \end{pmatrix}, \quad S_jT = \begin{pmatrix} F(z) + a \\ z \end{pmatrix},$$

et, par conséquent,

$$F(z+\beta) = F(z) + a;$$

si l'on remplace z successivement par $z+\beta$, $z+2\beta$, ...,

$z + Z\varepsilon$, il viendra

$$F(z + 2\varepsilon) = F(z + \varepsilon) + a = F(z) + 2a,$$
$$F(z + 3\varepsilon) = F(z + \varepsilon) + 2a = F(z) + 3a,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$F(z + Z\varepsilon) = F(z + \varepsilon) + (Z - 1)a = F(z) + Za;$$

enfin, si dans la dernière de ces égalités on pose $\varepsilon = 1$, $z = 0$, $F(0) = b$, on aura

$$F(Z) = aZ + b,$$

a et b étant des constantes. Ainsi le système G ne renferme que des substitutions de la forme

$$\begin{pmatrix} az + b \\ z \end{pmatrix}.$$

Cette conclusion s'applique en particulier au système qui est actuellement propre à l'équation.

589. Théorème II. — *Réciproquement, si le système* G *actuellement propre à l'équation irréductible* $f(x) = 0$ *de degré premier* n *ne renferme que des substitutions de la forme*

$$\begin{pmatrix} az + b \\ z \end{pmatrix},$$

l'équation est résoluble algébriquement.

En effet, désignons par α une racine de l'équation

$$(1) \qquad \frac{x^n - 1}{x - 1} = 0,$$

et par r une racine primitive pour le nombre premier n; posons en outre

$$(2) \quad \begin{cases} X_1 = (x_0 + \alpha x_1 + \alpha^2 x_2 + \ldots + \alpha^{n-1} x_{n-1})^n, \\ X_r = (x_0 + \alpha x_r + \alpha^2 x_{2r} + \ldots + \alpha^{n-1} x_{(n-1)r})^n \\ X_{r^2} = (x_0 + \alpha x_{r^2} + \alpha^2 x_{2r^2} + \ldots + \alpha^{n-1} x_{(n-1)r^2})^n, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots; \\ X_{r^{n-2}} = (x_0 + \alpha x_{r^{n-2}} + \alpha^2 x_{2r^{n-2}} + \ldots + \alpha^{n-1} x_{(n-1)r^{n-2}})^n. \end{cases}$$

Toute substitution du système G est le produit d'une puissance de la substitution

$$(3) \qquad \begin{pmatrix} z+1 \\ z \end{pmatrix}$$

par une puissance de la substitution

$$(4) \qquad \begin{pmatrix} rz \\ z \end{pmatrix}.$$

Les quantités

$$(5) \qquad X_1,\ X_r,\ X_{r^2},\ \ldots,\ X_{r^{n-2}}$$

sont invariables par la substitution (3) (n° 494), et elles sont déplacées circulairement par la substitution (4); donc toute fonction Ξ des quantités (5), qui reste invariable par la substitution (4) effectuée sur les indices des fonctions X, est une fonction des racines x_0, x_1, ..., x_{n-1} qui est invariable par les substitutions du système G; par conséquent (n° 578), cette fonction Ξ est rationnellement connue.

En particulier, si l'on désigne par λ une racine de l'équation

$$(6) \qquad x^{n-1} - 1 = 0$$

et que l'on fasse

$$(X_1 + \lambda X_r + \lambda^2 X_{r^2} + \ldots + \lambda^{n-2} X_{r^{n-2}})^{n-1} = \Xi,$$

la quantité Ξ sera connue; donc la quantité

$$X_1 + \lambda X_r + \lambda^2 X_{r^2} + \ldots + \lambda^{n-2} X_{r^{n-2}} = \sqrt[n-1]{\Xi}$$

sera elle-même connue après l'extraction d'une racine de degré $n-1$.

En prenant successivement pour λ chacune des racines de l'équation $x^{n-1} - 1 = 0$, on aura $n-1$ équations qui feront connaître les quantités (5); ensuite, si l'on extrait la racine $n^{\text{ième}}$ des équations (2), on aura un système de

$n-1$ équations du premier degré qui détermineront les n racines x, puisque la somme de ces racines est connue.

Ainsi l'équation proposée est résoluble algébriquement dans notre hypothèse.

590. Au moyen des théorèmes qui précèdent, Galois a pu énoncer, comme il suit, la condition de résolubilité des équations irréductibles de degré premier.

THÉORÈME III. — *Pour qu'une équation irréductible de degré premier soit résoluble par radicaux, il faut et il suffit que la résolvante de Lagrange ait une racine rationnelle.*

En effet, cette résolvante de degré $1, 2, 3, \ldots, (n-2)$ a pour racines les diverses valeurs que prend, par les substitutions des racines x, une fonction symétrique des quantités (5) du n° 589, par exemple la fonction

$$(X - X_1)(X - X_r)\ldots(X - X_{r^{n-2}}),$$

où X représente une indéterminée. Or il résulte des théorèmes I et II que, si la proposée est résoluble, cette quantité est connue quel que soit X ; donc la résolvante dont elle dépend doit avoir une racine rationnelle.

Réciproquement, si la résolvante a une racine rationnelle, la proposée est résoluble ; car, dans ce cas, la fonction que nous venons de considérer est connue, quel que soit X : c'est la racine rationnelle de la résolvante ; or cette fonction n'est invariable que par les seules substitutions de la forme $\left(\dfrac{az+b}{z}\right)$: donc le système propre à l'équation ne renferme que de telles substitutions (n° 583), et par conséquent (n° 589) l'équation proposée est résoluble.

591. La condition de résolubilité que nous venons de trouver peut encore être formulée d'une autre manière : tel est l'objet des propositions suivantes :

Théorème IV. — *Si une équation irréductible de degré premier est résoluble par radicaux, les racines sont toutes exprimables en fonction rationnelle de deux quelconques d'entre elles.*

En effet, d'après le théorème I, le système conjugué qui est actuellement propre à l'équation ne renferme que des substitutions de la forme $\begin{pmatrix} az+b \\ z \end{pmatrix}$. Or une telle substitution, qui ne se réduit pas à l'unité, déplace les n indices si $a=1$, et elle déplace $n-1$ indices si a est différent de 1. Il résulte de là que, si l'on adjoint à l'équation deux racines

$$x_\alpha, \; x_\beta,$$

le système propre à cette équation ne pourra plus contenir que la seule substitution égale à l'unité ; car, d'après le théorème du n° 583, les substitutions de ce système ne peuvent déplacer les indices α et β. Donc, les racines x_α et x_β étant regardées comme connues, toutes les autres racines sont en même temps rationnellement connues.

592. Théorème V. — *Réciproquement, si toutes les racines d'une équation irréductible de degré premier sont exprimables rationnellement en fonction de deux quelconques d'entre elles, l'équation est résoluble par radicaux.*

En effet, soient x_α, x_β deux racines quelconques de l'équation proposée

$$(1) \qquad f(x)=0.$$

Soient G le système conjugué actuellement propre à l'équation, Γ ce qu'il devient après l'adjonction de x_α et

avant celle de x_6. Soit aussi

$$(2) \qquad F(V) = 0$$

l'équation irréductible que nous avons nommée *résolvante* et dont le degré exprime l'ordre du système G.

L'équation (2) devient réductible par l'adjonction de x_α, car soit V_0 l'une de ses racines, x_α est exprimable en fonction rationnelle de V_0; et si l'on pose

$$x_\alpha = \psi(V_0),$$

on pourra supposer (n° 182) que ψ soit une fonction entière de degré inférieur à F (V). La racine V_0 est ainsi commune à l'équation

$$\psi(V) - x_\alpha = 0$$

et à l'équation (2); par conséquent celle-ci cesse d'être irréductible. Mais alors la réduction s'opère (n° 580) par la décomposition de F(V) en p facteurs du même degré, p étant un diviseur du degré de l'équation auxiliaire irréductible dont dépend la racine adjointe. Ici cette équation auxiliaire n'est autre que la proposée elle-même dont le degré est le nombre premier n; par conséquent on a $p = n$. Ainsi l'ordre du système Γ est la $n^{\text{ième}}$ partie de l'ordre G.

Passons à l'adjonction de la racine x_6. La racine x_α faisant actuellement partie des quantités connues, la racine x_6, qu'il reste à adjoindre, est racine d'une équation irréductible

$$(3) \qquad f_1(x, x_\alpha) = 0,$$

dont le premier membre est égal au quotient $\dfrac{f(x)}{x - x_\alpha}$ ou à un diviseur rationnel de ce quotient, et, par hypothèse, l'adjonction de x_6 doit réduire à l'unité le système propre à l'équation, lequel est actuellement Γ. Mais, en vertu

du théorème du n° 580, par l'adjonction dont il s'agit, l'ordre du système propre à l'équation est divisé par un facteur m du degré de l'équation auxiliaire, lequel est au plus égal à $n - 1$; donc l'ordre de Γ est égal à m, et par suite l'ordre de G est égal à nm.

Le système G ne peut renfermer une substitution qui laisserait deux indices immobiles, car, les racines étant exprimables rationnellement par deux quelconques d'entre elles, supposons que l'on ait

$$x_\gamma = \varphi(x_\alpha, x_\beta), \quad x_\delta = \chi(x_\alpha, x_\beta), \quad x_\varepsilon = \varpi(x_\alpha, x_\beta), \quad \ldots;$$

les différences

$$x_\gamma - \varphi(x_\alpha, x_\beta), \quad x_\delta - \chi(x_\alpha, x_\beta), \quad \ldots$$

sont actuellement connues, puisqu'elles sont nulles; or une substitution autre que l'unité, qui laisserait immobiles les indices α et β, ferait varier quelques-unes de ces différences. Une telle substitution ne peut donc appartenir à G (n° 578), et, par suite, à Γ.

Maintenant le système Γ se compose de celles des substitutions de G qui ne déplacent pas l'indice α (n° 583); donc il y a dans G, outre l'unité, $m - 1$ substitutions qui laissent l'indice α immobile, et, comme on peut en dire autant des autres indices, on voit que le système G renferme $(m-1)n+1$ ou $mn-(n-1)$ substitutions qui ne déplacent pas simultanément les n indices. Donc le nombre des substitutions de G qui déplacent tous les indices est égal à $n - 1$; je dis que ces substitutions sont circulaires et puissances les unes des autres. En effet, soit T l'une de ces substitutions; décomposons-la en cycles, et soit

$$T = C_1 C_2 C_3 \ldots;$$

l'ordre de T est un diviseur de nm; si donc T ne se réduit pas à un cycle unique d'ordre n, l'ordre de cette substitution sera égal à un diviseur d de m. Dans notre

hypothèse la substitution T déplace toutes les racines : elle n'a donc pas de cycles du premier ordre, et elle est irrégulière, puisque le nombre n des lettres est premier. Soit δ l'ordre du cycle le moins élevé ; la substitution T^δ laissera deux lettres au moins immobiles : donc elle ne peut appartenir à G ; par conséquent la substitution T ne peut elle-même faire partie de G.

Ainsi le système G renferme une substitution circulaire T de l'ordre n, et les puissances de T sont les seules substitutions de G qui déplacent tous les indices. Alors, si l'on désigne par

$$(1) \qquad 1,\ S_1,\ S_2\ \ldots,\ S_{m-1}$$

les substitutions de Γ, on obtiendra le système G en multipliant les substitutions (1), soit à droite, soit à gauche, par le système conjugué

$$(2) \qquad 1,\ T,\ T^2,\ \ldots,\ T^{n-1},$$

formé des puissances de T. Deux des produits ainsi obtenus sont en effet distincts et ils font partie de G.

Cela étant, on peut distribuer les indices 0, 1, 2, ... des lettres x de manière que la substitution T soit

$$T = \begin{pmatrix} z+1 \\ z \end{pmatrix}.$$

Désignons alors par

$$U = \begin{pmatrix} F(z) \\ z \end{pmatrix}$$

une substitution quelconque de G ; la substitution UTU^{-1} semblable à T fait partie de G, elle est circulaire, et elle coïncide, d'après ce qui précède, avec l'une des puissances de T ; ainsi l'on a

$$UTU^{-1} = T^a \quad \text{ou} \quad UT = T^a U,$$

a étant un exposant convenable. Cette égalité revient

$$F(z+1) = F(z) + a;$$

remplaçant successivement z par $z+1$, $z+2$, ..., $z+Z$, on trouve

$$F(z+Z) = F(z) + aZ;$$

faisant enfin $z = 0$, $F(0) = b$, il vient

$$F(Z) = aZ + b:$$

ainsi le système G ne renferme que des substitutions de la forme $az+b$; donc l'équation proposée est résoluble d'après le théorème II.

593. La théorie que nous venons d'exposer fournit une démonstration nouvelle de l'impossibilité de résoudre algébriquement les équations générales au delà du quatrième degré. Effectivement, dans le cas de l'équation générale du cinquième degré, la condition du théorème IV n'est pas remplie, et par conséquent l'équation n'est pas résoluble. L'impossibilité de résoudre l'équation générale du cinquième degré entraîne d'ailleurs la même impossibilité à l'égard des équations générales de degré plus élevé.

Recherches de M. Hermite.

594. Il ne sera pas inutile de présenter ici une analyse remarquable que M. Hermite m'a communiquée, et qui a pour objet la démonstration de ce théorème de Galois :

Étant données deux quelconques des racines d'une équation irréductible de degré premier, soluble par radicaux, les autres s'en déduisent rationnellement.

Lemme I. — *Soient*

$$F(x) = 0$$

une équation irréductible de degré quelconque n, *et*

$$x_0,\ x_1,\ x_2,\ \ldots,\ x_{n-1}$$

ses n *racines. Si toutes les fonctions des racines in-*

variables par les substitutions de la forme x_k, x_{k+1} *ou* $\binom{k+1}{k}$ (les indices étant pris comme fait Galois, suivant le module n) *sont rationnellement connues, on pourra déterminer rationnellement une fonction entière* $\varphi(x)$ *du degré* $n-1$, *telle que l'on ait*

$$x_1=\varphi(x_0),\ x_2=\varphi(x_1),\ \ldots,\ x_{k+1}=\varphi(x_k),\ \ldots,\ x_{n-1}=\varphi(x_{n-2}).$$

On a, en effet,

$$F(x)=(x-x_0)(x-x_1)\ \ldots\ (x-x_{n-1}),$$

et, si l'on pose

$$\varphi(x)=\frac{F(x)}{x-x_0}\frac{x_1}{F'(x_0)}+\frac{F(x)}{x-x_1}\frac{x_2}{F'(x_1)}+\ldots+\frac{F(x)}{x-x_{n-1}}\frac{x_0}{F'(x_{n-1})},$$

il est évident que $\varphi(x)$ sera une fonction entière du degré $n-1$ en x et que ses coefficients seront des fonctions des racines invariables par les substitutions de la forme x_k, x_{k+1}; on voit aussi immédiatement que l'on a

$$\varphi(x_0)=x_1,\quad \varphi(x_1)=x_2,\quad \ldots,$$

ce qui démontre la proposition énoncée.

595. Lemme II. — *Si une équation irréductible de degré premier* n *est telle, que toutes les fonctions des racines invariables par les substitutions de la forme* x_k, x_{k+1}, *et de la forme* $x_k, x_{\rho k}$, ρ *désignant une racine primitive de* n, *soient rationnellement connues, on pourra déterminer rationnellement une fonction entière de* $\varphi(x)$ *de degré* $n-1$, *telle que l'on ait*

$$\begin{aligned}
(x_1+\lambda x_\rho\quad &+\lambda^2 x_{\rho^2}\quad +\ldots+\lambda^{n-2}x_{\rho^{n-2}}\quad)^{n-1}=\varphi(x_0),\\
(x_2+\lambda x_{\rho+1}\quad &+\lambda^2 x_{\rho^2+1}\quad +\ldots+\lambda^{n-2}x_{\rho^{n-2}+1}\quad)^{n-1}=\varphi(x_1),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
(x_n+\lambda x_{\rho+n-1}&+\lambda^2 x_{\rho^2+n-1}+\ldots+\lambda^{n-2}x_{\rho^{n-2}+n-1})^{n-1}=\varphi(x_{n+1});
\end{aligned}$$

les indices étant pris toujours suivant le module n et λ désignant une racine de l'équation binôme $\lambda^{n-1} = 1$.

Pour démontrer cette proposition, nous ferons voir que le système des équations linéaires ainsi posées entre les coefficients indéterminés de la fonction φ n'est pas altéré lorsqu'à la place d'une racine quelconque x_k on met x_{k+1} et aussi quand on remplace x_k par $x_{\rho k}$.

Le premier point est évident, puisque chaque équation se déduit de la précédente en ajoutant une unité aux indices des racines, et qu'en opérant de la sorte sur la dernière on reproduit la première.

Le second point se vérifie aussi immédiatement par rapport à l'équation

$$(x_1 + \lambda x_\rho + \lambda^2 x_{\rho^2} + \ldots + \lambda^{n-2} x_{\rho^{n-2}})^{n-1} = \varphi(x_0),$$

car la $(n-1)^{\text{ième}}$ puissance de la fonction linéaire

$$x_1 + \lambda x_\rho + \lambda^2 x_{\rho^2} + \ldots + \lambda^{n-2} x_{\rho^{n-2}}$$

ne change pas quand on multiplie cette fonction par λ; or cela revient à multiplier les indices des racines par ρ, ce qui ne change pas non plus le second membre $\varphi(x_0)$. Mais les autres équations du système ne se comportent plus de même. Dans l'une quelconque d'entre elles

$$(x_{1+\alpha} + \lambda x_{\rho+\alpha} + \lambda^2 x_{\rho^2+\alpha} + \ldots + \lambda^{n-2} x_{\rho^{n-2}+\alpha})^{n-1} = \varphi(x_\alpha),$$

faisons $\alpha \equiv \rho^\mu \pmod{n}$, ce qui est possible, puisque α ne reçoit plus la valeur zéro; il viendra

$$(1)\quad (x_{1+\rho^\mu} + \lambda x_{\rho+\rho^\mu} + \lambda^2 x_{\rho^2+\rho^\mu} + \ldots + \lambda^{n-2} x_{\rho^{n-2}+\rho^\mu})^{n-1} = \varphi(x_{\rho^\mu}),$$

et, en multipliant les indices par ρ,

$$(2)\quad (x_{\rho+\rho^{\mu+1}} + \lambda x_{\rho^2+\rho^{\mu+1}} + \lambda^2 x_{\rho^3+\rho^{\mu+1}} + \ldots + \lambda^{n-2} x_{\rho^{n-1}+\rho^{\mu+1}})^{n-1} = \varphi(x_{\rho^{\mu+1}}).$$

Or la $(n-1)^{\text{ième}}$ puissance de la fonction linéaire

$$x_{\rho+\rho^{\mu+1}} + \lambda x_{\rho^2+\rho^{\mu+1}} + \ldots + \lambda^{n-1} x_{\rho^{n-1}+\rho^{\mu+1}}$$

ne change pas quand on multiplie cette fonction par λ; au lieu de l'équation (2), on peut donc écrire la suivante:

$$(x_{\rho^{n-1}+\rho^{\mu+1}} + \lambda x_{\rho+\rho^{\mu+1}} + \lambda^2 x_{\rho^2+\rho^{\mu+1}} + \ldots \\ + \lambda^{n-2} x_{\rho^{n-2}+\rho^{\mu+1}})^{n-1} = \varphi(x_{\rho^{\mu+1}}).$$

Or, en remarquant que $\rho^{n-1} \equiv 1 \pmod{n}$, on reconnaît que celle-ci se déduit de l'équation (1) par le changement de μ en $\mu+1$.

Il suit de là que la substitution $x_k, x_{\rho k}$ ne fait que permuter circulairement nos équations, rangées, à partir de la deuxième, suivant l'ordre des valeurs croissantes de μ. En les résolvant par rapport aux coefficients de φ, on sera conduit à des fonctions rationnelles des racines, invariables par les substitutions x_k, x_{k+1} et $x_k, x_{\rho k}$; de sorte que ces coefficients s'exprimeront bien rationnellement, comme nous l'avons annoncé. Notre lemme est donc démontré, et l'on en déduit le suivant :

596. Lemme III. — *Si une équation de degré premier est résoluble algébriquement, l'équation de degré moindre d'une unité, qu'on forme en divisant son premier membre par un de ses facteurs linéaires, appartient à la classe des équations abéliennes.*

En effet, relativement à l'équation de degré $n-1$, qu'on obtient par la suppression du facteur $x - x_\alpha$, et dont les racines ont été représentées par

$$x_{1+\alpha}, \quad x_{\rho+\alpha}, \quad x_{\rho^2+\alpha}, \quad \ldots, \quad x_{\rho^{n-2}+\alpha},$$

on connaît *rationnellement* la fonction résolvante

$$(x_{1+\alpha} + \lambda x_{\rho+\alpha} + \lambda^2 x_{\rho^2+\alpha} + \ldots + \lambda^{n-2} x_{\rho^{n-2}+\alpha})^{n-1}.$$

597. Les trois lemmes que nous venons de démontrer permettent maintenant d'établir très-aisément le théorème que nous avons en vue. Faisons pour un instant

$$x_{\rho^k+\alpha} = X_k.$$

Puisque nous connaissons (lemme III), en fonction rationnelle de x_α, l'expression

$$(X_0 + \lambda X_1 + \lambda^2 X_2 + \ldots + \lambda^{n-2} X_{n-2})^{n-1},$$

nous devons pareillement regarder comme connue toute fonction rationnelle des racines X_k, invariable par les substitutions de la forme X_k, X_{k+1}. Cela nous place dans les conditions du lemme I; ainsi nous pouvons former une fonction φ telle qu'on ait généralement

$$X_{k+1} = \varphi(X_k).$$

D'ailleurs, les coefficients de cette fonction s'exprimeront rationnellement par les quantités connues et la racine x_α; de sorte qu'en mettant cette racine en évidence nous aurons

$$X_{k+1} = \varphi(X_k, x_\alpha), \quad \text{ou} \quad x_{\rho^{k+1}+\alpha} = \varphi(x_{\rho^k+\alpha}, x_\alpha).$$

Or on peut prendre $\rho^k = 6$, 6 étant un entier arbitraire, mais essentiellement différent de zéro; il vient ainsi

$$x_{\rho 6+\alpha} = \varphi(x_{6+\alpha}, x_\alpha).$$

Cette équation exprime précisément la relation que nous nous proposions d'établir; elle montre très-facilement comment toutes les racines s'expriment de proche en proche, au moyen des deux racines arbitraires x_α, $x_{\alpha+6}$, et met immédiatement en évidence dans quel ordre elles naissent ainsi les unes des autres.

598. Il est aisé de démontrer que, réciproquement, la

relation précédente, admise entre trois racines x_α, $x_{\alpha+\beta}$, $x_{\alpha+\rho\beta}$, entraîne la résolution par radicaux de l'équation.

A cet effet, soient θ une racine de l'équation binôme $x^n = 1$, et

$$F(\theta) = (x_0 + \theta x_1 + \theta^2 x_2 + \ldots + \theta^{n-1} x_{n-1})^n$$

la fonction résolvante de Lagrange. D'après la propriété caractéristique de cette fonction, on pourra, sans altérer sa valeur, ajouter aux indices des racines un nombre entier arbitraire α, et écrire

$$F(\theta) = (x_\alpha + \theta x_{\alpha+1} + \theta^2 x_{\alpha+2} + \ldots + \theta^{n-1} x_{\alpha+n-1})^n.$$

Cela posé, soit β un autre nombre entier arbitraire, mais différent de zéro, et prenons β_0 de manière qu'on ait

$$\beta\beta_0 \equiv 1 \quad (\text{mod. } n);$$

on voit immédiatement que l'on a

$$F(\theta^{\beta_0}) = (x_\alpha + \theta x_{\alpha+\beta} + \theta^2 x_{\alpha+2\beta} + \ldots + \theta^{n-1} x_{\alpha+(n-1)\beta})^n,$$

et il est clair qu'en employant la relation

$$x_{\rho\beta+\alpha} = \varphi(x_{\beta+\alpha}, x_\alpha)$$

on pourra, par des substitutions successives, transformer le second membre en une fonction rationnelle Π des deux racines x_α, $x_{\alpha+\beta}$, de manière à avoir

$$F(\theta^{\beta_0}) = \Pi(x_\alpha, x_{\alpha+\beta})$$

pour une valeur quelconque de l'indice arbitraire α.

Cela étant, soit, comme plus haut, λ une racine de l'équation binôme $x^{n-1} = 1$, la fonction

$$[\Pi(x_\alpha, x_{\alpha+\beta}) + \lambda \Pi(x_\alpha, x_{\alpha+\rho\beta}) + \lambda^2 \Pi(x_\alpha, x_{\alpha+\rho^2\beta}) + \ldots + \lambda^{n-2} \Pi(x_\alpha, x_{\alpha+\rho^{n-2}\beta})]^{n-1}$$

conserve la même valeur quand on met $\rho\beta$ au lieu de β,

c'est-à-dire qu'elle est indépendante de la valeur attribuée à β. Chacun des termes dont elle se compose est d'ailleurs indépendant de α; donc, en la transformant, au moyen de la relation

$$x_{\alpha+\rho\beta} = \varphi(x_{\alpha+\beta}, x_\alpha),$$

en une fonction rationnelle des deux seules racines x_α et $x_{\alpha+\beta}$, cette fonction devra se réduire à une quantité connue. Effectivement, si une fonction

$$u = \psi(x_{\alpha+\beta}, x_\alpha)$$

conserve la même valeur, quels que soient les indices α et β, le second indice étant différent de zéro, on peut écrire

$$n(n-1)u = \sum_{0}^{n-1}{}_{\alpha} \sum_{1}^{n-1}{}_{\beta} \psi(x_{\alpha+\beta}, x_\alpha),$$

relation dont le second membre est une fonction symétrique de toutes les racines $x_0, x_1, \ldots, x_{n-1}$.

Il résulte de là que nous pouvons regarder les $n-1$ quantités

$$\Pi(x_\alpha, x_{\alpha+\beta}), \quad \Pi(x_\alpha, x_{\alpha+\rho\beta}), \quad \ldots, \quad \Pi(x_\alpha, x_{\alpha+\rho^{n-2}\beta})$$

comme les racines d'une équation abélienne résoluble par l'extraction d'un seul radical de degré $n-1$. Or, ces quantités une fois obtenues, nous connaissons, pour toutes les valeurs de β, excepté $\beta = 0$, la puissance $n^{\text{ième}}$ de la fonction résolvante $F(\theta^{\beta_0})$; donc, par l'extraction de $n-1$ radicaux du $n^{\text{ième}}$ degré, nous aurons ces diverses fonctions résolvantes, et, par conséquent, les racines elles-mêmes. On sait d'ailleurs, par une observation d'Abel, que ces $n-1$ radicaux s'expriment rationnellement en fonction de l'un d'entre eux et des quantités sur

lesquelles ils portent, quantités qui sont, comme nous venons de le dire, les racines d'une équation abélienne.

Recherches de M. Kronecker.

599. Je reproduirai ici, en terminant cet Ouvrage, la traduction textuelle d'un Mémoire de M. Léopold Kronecker, communiqué par Lejeune-Dirichlet à la classe des Sciences mathématiques et physiques de l'Académie de Berlin, le 20 juin 1853 :

« Les recherches entreprises jusqu'à présent sur la possibilité de résoudre les équations de degré premier, et particulièrement celles d'Abel et de Galois qui ont servi de point de départ à tous les travaux ultérieurs sur le même objet, ont eu pour principal résultat de conduire à deux critérium à l'aide desquels on pût juger si une équation donnée est résoluble ou non. Mais, à vrai dire, ces critérium ne fournissaient pas la moindre lumière sur la nature même des équations résolubles. On ne savait même pas si, en outre des équations traitées par Abel dans le tome IV du *Journal de Crelle*, et de celles qui se ramènent immédiatement aux équations binômes, on ne savait pas, dis-je, s'il existait d'autres équations satisfaisant aux conditions données de résolubilité. Encore moins savait-on former de pareilles équations, et dans aucune recherche mathématique on n'en avait rencontré. Ajoutons que ces deux théorèmes bien connus d'Abel et de Galois sur les équations résolubles étaient plus propres à en cacher la vraie nature qu'à nous la découvrir, ainsi que je le montrerai plus particulièrement à l'égard de l'un de ces critérium. Le caractère propre des équations résolubles restait donc dans une sorte d'obscurité, et le seul travail qui jette quelque lumière sur ce point, savoir : une Notice d'Abel sur les racines

des équations du cinquième degré à coefficients entiers, semble avoir été peu remarqué, sans doute à cause de son objet tout spécial. Mais la question ne pouvait être complétement éclaircie que par la solution du problème suivant : *Trouver toutes les équations résolubles.* Car, une fois cette solution obtenue, non-seulement on peut trouver une infinité de nouvelles équations résolubles, mais on a en quelque sorte devant les yeux toutes celles qui le sont, et à l'aide de la forme explicite de leurs racines on peut trouver et démontrer toutes leurs propriétés.

» A ces remarques sur le but et le résultat de mes recherches, je dois ajouter que, pour rendre la solution possible, il fallait encore transformer complétement le problème qui vient d'être posé. La manière de formuler la question est, en effet, de la plus grande importance, et, de peur que la brièveté ne nuise à la clarté, je m'étendrai un peu sur ce point.

» Abel, dans un Mémoire dont nous ne possédons que des fragments (t. II, *OEuvres complètes,* n° XV), s'est proposé, entre autres problèmes, celui-ci : *Trouver l'expression algébrique la plus générale qui puisse satisfaire à une équation algébrique d'un degré donné. Si l'on* ajoute à cet énoncé ce qui est nécessaire pour rendre la question déterminée, il comprend tous les problèmes qu'on peut se proposer sur la résolution des équations, et il est le plus général qu'on doive substituer à ce problème impossible : *Exprimer en fonction algébrique des coefficients la racine d'une équation de degré quelconque.* Mais, ainsi qu'on vient de le dire, il fallait rendre la question déterminée en précisant la manière dont l'expression cherchée doit dépendre des coefficients de l'équation ; il convient donc de la poser comme il suit :

» *Trouver la fonction la plus générale de quantités données quelconques* A, B, C, ..., *qui satisfasse à une*

équation d'un degré donné dont les coefficients sont des fonctions rationnelles de ces quantités.

» Observons qu'on doit supposer ici l'équation irréductible relativement à A, B, C, ..., c'est-à-dire que, A, B, C, ... restant quelconques, l'équation ne doit pas pouvoir se décomposer en facteurs d'un degré moindre dont les coefficients soient des fonctions rationnelles de A, B, C, ... Cela posé, le problème précédent peut s'énoncer de cette manière :

» *Étant donné un nombre entier n, trouver la fonction algébrique la plus générale de* A, B, C, ... *telle que, parmi les expressions qu'on en déduit en attribuant aux radicaux leurs diverses valeurs, il y en ait n dont les fonctions symétriques soient rationnelles en* A, B, C, ...

» Ce nombre n est aussi le degré de l'équation qui a pour racines les n expressions dont on vient de parler : dans le cas où il est le premier, Abel, dans le Mémoire cité, est parvenu à donner les deux formes suivantes aux expressions algébriques cherchées. La première est

$$(1) \qquad p_0 + s^{\frac{1}{\mu}} + f_2(s)\, s^{\frac{2}{\mu}} + \ldots + f_{\mu-1}(s)\, s^{\frac{\mu-1}{\mu}}$$

(tome II des *Œuvres complètes*, p. 204), où μ désigne le degré supposé premier de l'équation, p_0 une fonction rationnelle de A, B, C, ..., s une fonction algébrique des mêmes quantités, et $f_k(s)$ une fonction rationnelle de s et de A, B, C, ... La seconde forme, qu'on trouve à la page 190 du même volume, est

$$(2) \qquad p_0 + R_1^{\frac{1}{\mu}} + R_2^{\frac{1}{\mu}} + \ldots + R_{\mu-1}^{\frac{1}{\mu}},$$

où p_0 est une fonction rationnelle de A, B, C, ... et où R_1, R_2, ... sont les racines d'une équation du degré

$\mu - 1$ dont les coefficients sont des fonctions rationnelles de A, B, C, ... M. Malmsten a donné de ces deux formes une démonstration étendue (t. XXXIV du *Journal de Crelle*), mais qui aurait besoin, si je ne me trompe, d'être complétée dans quelques-unes de ses parties.

» Il est bien vrai que toute fonction algébrique, satisfaisant au problème proposé, doit pouvoir se mettre sous ces deux formes; mais ces formes sont encore trop générales, c'est-à-dire qu'elles renferment des fonctions algébriques qui ne répondent pas à la question. Je les ai donc étudiées de plus près, et j'ai trouvé d'abord que, parmi les fonctions renfermées dans la forme (2), celles qui satisfont au problème proposé doivent avoir la propriété non-seulement que les fonctions symétriques de R_1, R_2, ... soient rationnelles en A, B, C, ... (ce qu'Abel a remarqué), mais aussi que les fonctions cycliques des quantités R_1, R_2, ..., prises dans un certain ordre ([1]), soient également rationnelles en A, B, C, ... : en d'autres termes, *l'équation de degré* $\mu - 1$, *dont* R_1, R_2, ... *sont les racines, doit être une équation abélienne.* J'entendrai toujours ici par équations abéliennes cette classe particulière d'équations résolubles qu'Abel a considérées dans le Mémoire XI du premier volume des *Œuvres complètes*, et dont je supposerai les coefficients fonctions rationnelles de A, B, C, ... En désignant par x_1, x_2, ..., x_n des racines prises dans un ordre déterminé, ces équations peuvent être définies soit en disant que les fonctions cycliques des racines sont rationnelles en A, B, C, ..., soit en disant qu'on a les relations

$$x_2 = \theta(x_1), \quad x_3 = \theta(x_2), \quad \ldots, \quad x_n = \theta(x_{n-1}), \quad x_1 = \theta(x_n),$$

([1]) On nomme fonction *cyclique* de n quantités x_1, x_2, ..., x_n l'expression $(x_1 + \alpha x_2 + \alpha^2 x_3 + \ldots + \alpha^{n-1} x_n)^n$, où α est racine de $\alpha^n = 1$.

où $\theta(x)$ est une fonction entière de x dont les coefficients sont rationnels en A, B, C, ... Nous reviendrons tout à l'heure sur ces équations, dont la considération est du plus haut intérêt au point de vue de l'analyse et de la théorie des nombres, et aussi, comme on le voit, au point de vue de l'Algèbre proprement dite.

» Un nouvel examen des formes (1) et (2) fournit encore une détermination plus précise des quantités R qui figurent dans la seconde. On doit avoir, en effet,

$$(3) \qquad R_x = F(r_x)^{\mu} r_x^{\gamma-1} r_{x+1}^{\gamma-2} r_{x+2}^{\gamma-3} \ldots r_{x+\mu-2},$$

où r_x, r_{x+1}, ... sont les $\mu - 1$ racines d'une équation abélienne quelconque du degré $\mu - 1$, c'est-à-dire où les fonctions symétriques et les fonctions cycliques des quantités r (prises dans l'ordre des indices) sont rationnelles en A, B, C, ... où, de plus, $F(r)$ est une fonction rationnelle de r et de A, B, C, ... et où enfin γ_m désigne le plus petit reste positif de g^m suivant le module μ, g étant une racine primitive de μ. Si l'on substitue cette valeur de R_x dans l'expression (2), on obtient une forme qui, non-seulement renferme toutes les expressions satisfaisant au problème, mais, ce qui est ici le plus essentiel, n'en renferme pas d'autres. En d'autres termes, la forme ainsi obtenue vérifie identiquement une équation du degré μ dont les coefficients sont des fonctions rationnelles de A, B, C, ... Les autres racines s'obtiennent par la combinaison des diverses valeurs des radicaux $\mu^{\text{ièmes}}$ dans la forme (2), de façon que la $m^{\text{ième}}$ racine z_m est donnée par la formule

$$(4) \quad z_m = p_0 + \omega^{m} R_1^{\frac{1}{\mu}} + \omega^{gm} R_2^{\frac{1}{\mu}} + \omega^{g^2.m} R_3^{\frac{1}{\mu}} + \ldots + \omega^{g^{\mu-2}.m} R_{\mu-1}^{\frac{1}{\mu}},$$

ω désignant une racine $\mu^{\text{ième}}$ imaginaire de l'unité, et les quantités R étant déterminées par la formule (3).

» De là il suit d'abord que, tandis que les fonctions symétriques des quantités z sont rationnelles en A, B, C, ..., les fonctions cycliques des mêmes quantités prises dans l'ordre des indices sont des fonctions rationnelles de A, B, C, ..., de r_1, r_2, ..., et de ω. On voit par là que *toute équation résoluble algébriquement d'un degre premier μ est une équation abélienne, quand on regarde comme connue une quantité ρ_1 qui elle-même est racine d'une équation abélienne du degré $\mu - 1$*, ou bien encore que *les μ racines d'une équation résoluble sont toujours liées entre elles de façon que l'on ait*

$$z_2 = f(z_1, \rho_1), \quad z_3 = f(z_2, \rho_1), \quad \ldots, \quad z_1 = f(z_\mu, \rho_1),$$

où $f(z, \rho_1)$ désigne une fonction rationnelle de z, de ρ_1 et de A, B, C, ... (¹), *et où ρ_1 est la racine d'une équation abélienne dont les coefficients sont des fonctions rationnelles de* A, B, C, ... Cette relation entre les racines de toute équation résoluble est d'ailleurs la vraie source de la propriété assignée par Abel et Galois comme le caractère spécial des équations résolubles d'un degré premier, savoir : *que chaque racine doit être une fonction rationnelle des deux autres*. Parmi les conséquences intéressantes qui découlent des résultats précédents, je me bornerai à une seule : c'est que, la quantité r_1 étant racine d'une équation abélienne du degré $\mu - 1$ et ne contenant que des radicaux dont les indices sont diviseurs de $\mu - 1$ ou pouvant être ramenée à n'en contenir que de tels, la racine elle-même de toute équation résoluble

(¹) J'ai fait dans ce passage quelques corrections qui m'ont été indiquées par M. Kronecker lui-même. La quantité que nous représentons ici par ρ_1 se trouve désignée, à tort, dans les *Comptes rendus de l'Académie des Sciences de Berlin*, par la lettre r_1. Cette nouvelle racine ρ_1 dépend de la racine r_1 d'une manière très-simple ; toutefois ces deux quantités sont différentes entre elles.

pourra s'exprimer par les radicaux dont on vient de parler et par des radicaux d'indice μ. Abel (autant que je le sache) n'a fait cette importante remarque que pour $\mu=5$, et, pour ce cas, il a donné la forme la plus générale de la racine d'une équation résoluble (t. II des *OEuvres complètes*, p. 253). Mais il faut observer qu'il s'est borné, dans cette recherche, aux équations dont les coefficients sont des nombres entiers.

» Le problème primitif est maintenant ramené, en vertu de l'équation (3), à trouver la forme la plus générale de la quantité ou, pour mieux dire, de l'expression r_1. D'après ce qu'on a établi ci-dessus au sujet de r_1, r_2, ..., ce second problème peut s'énoncer ainsi :

» *Le nombre n étant donné, trouver la forme la plus générale d'une fonction algébrique de* A, B, C, ..., *telle que, parmi les diverses expressions qui résultent de la combinaison des valeurs des radicaux dans cette fonction, il y en ait n dont les fonctions symétriques et cycliques (celles-ci étant relatives à un ordre déterminé des n expressions) soient rationnelles en* A, B, C, ...

» Et l'on voit que ce second problème, énoncé en gros pour ainsi dire, revient *à trouver toutes les équations abéliennes,* comme le problème primitif consistait, en quelque sorte, *à trouver toutes les équations résolubles.*

» En traitant ce second problème, on se trouve ramené à distinguer les cas où n est un nombre premier, ou une puissance de nombre premier, ou un nombre composé quelconque ; mais ce dernier cas se ramène aux deux autres, car la solution du problème pour un nombre composé n s'obtient dès qu'on l'a résolu pour les cas où le degré de l'équation abélienne est une des puissances de nombre premier contenues dans n. D'ailleurs, à part quelques complications, le problème n'offre pas plus de

difficultés pour une puissance de nombre premier que pour un nombre premier. Seulement, dans le cas le plus simple en apparence, où n est égal au cube ou à une puissance plus élevée de 2, la méthode que j'ai employée avec succès dans tous les autres cas ne suffit plus à la solution complète du problème, et je n'ai pas encore trouvé la modification qu'elle exige alors. Comme la solution du problème primitif pour le nombre premier μ exige la solution du second problème pour $n = \mu - 1$, je ne pourrais donc, jusqu'à présent, donner le résultat complet que pour les nombres premiers μ qui ne sont pas de la forme $8h + 1$. Il suffira, du reste, au but de cette communication préliminaire et pour éclaircir la matière, d'examiner ici le cas du second problème, où n est un nombre premier impair. Je ne donnerai pas seulement le résultat relatif à ce cas, mais j'indiquerai brièvement la méthode qui m'y a conduit, attendu qu'elle est extrêmement simple et qu'elle fournit les principes essentiels pour la solution de ce second problème dans les autres cas, et aussi pour la solution du problème primitif.

» En conservant les notations employées par Abel (dans le Mémoire n° XI déjà cité du tome Ier des *Œuvres complètes*), et en ayant égard à la définition déjà donnée des équations abéliennes, on peut énoncer comme il suit le problème dont il s'agit :

» *Trouver la fonction algébrique la plus générale* z_0 *de* A, B, C, ..., *satisfaisant à une équation du* $n^{ième}$ *degré, et telle que cette fonction* z_0 *et les autres racines* z_1, z_2, ..., z_{n-1} *de l'équation vérifient les relations*

$$z_1 = \theta(z_0), \quad z_2 = \theta(z_1), \quad \ldots, \quad z_0 = \theta(z_{n-1}),$$

où $\theta(z)$ *est une fonction rationnelle de* z *et de* A, B, C, ...

» Admettons que n soit un nombre premier, et, adop-

tant une notation introduite par M. Jacobi, posons

$$z_0 + z_1\alpha + z_2\alpha^2 + \ldots + z_{n-1}\alpha^{n-1} = (\alpha, z),$$

où α désigne une racine $n^{\text{ième}}$ de l'unité; nous aurons

$$(5)\quad nz_x = (1, z) + \alpha^{-x}(\alpha, z) + \alpha^{-2x}(\alpha^2, z) + \ldots + \alpha^{-(n-1)x}(\alpha^{n-1}, z).$$

En suivant la marche tracée par Abel, on montrera ensuite que, pour tout nombre entier x, on a les équations

$$(6)\quad \begin{cases} (\alpha, z)^x = (\alpha^x, z)\varphi(\alpha), \quad (\alpha^2, z)^x = (\alpha^{2x}, z)\varphi(\alpha^2), \\ (\alpha^3, z)^x = (\alpha^{3x}, z)\varphi(\alpha^3), \ldots, \end{cases}$$

où $\varphi(\alpha)$ est une fonction rationnelle de α et de A, B, C, ...

» Si maintenant on met pour x une racine primitive g du nombre premier n, tellement choisie que $g^{n-1} - 1$ ne soit divisible par aucune puissance de n plus élevée que la première, on obtiendra des équations de cette forme

$$(\alpha, z)^g = (\alpha^g, z)f(\alpha), \quad (\alpha^g, z)^g = (\alpha^{g^2}, z)f(\alpha^g), \quad \ldots,$$
$$(\alpha^{g^{n-2}}, z)^g = (\alpha, z)\, f(\alpha^{g^{n-2}}).$$

Élevons la première de ces équations à la puissance g^{n-2}, la seconde à la puissance g^{n-3}, et ainsi de suite, puis multiplions-les membre à membre; il viendra

$$(7)\quad (\alpha, z)^{g^{n-1}-1} = f(\alpha)^{g^{n-2}} f(\alpha^g)^{g^{n-3}} \ldots f(\alpha^{g^{n-2}}).$$

Posons à présent

$$g^{n-1} - 1 = mn,$$

m n'étant pas divisible par n, d'après la supposition précédemment faite; nous aurons, en vertu de l'équation (6),

$$(\alpha, z)^{g^{n-1}-1} = (\alpha, z)^{mn} = (\alpha^m, z)^n \varphi(\alpha)^n,$$

et, en substituant dans l'équation (7), nous trouverons

$$(\alpha^m, z)^n \varphi(\alpha)^n = f(\alpha)^{g^{n-2}} f(\alpha^g)^{g^{n-3}} \ldots f(\alpha^{g^{n-2}}),$$

résultat qui subsiste pour chacune des valeurs de α, comme on peut le démontrer, et qu'on mettra aisément sous cette forme

$$8)\quad (\alpha^m, z) = F(\alpha^m) \left\{ f(\alpha^m) f(\alpha^{2m})^{\frac{1}{2}} f(\alpha^{3m})^{\frac{1}{3}} \ldots f[\alpha^{(n-1)m}]^{\frac{1}{n-1}} \right\}^{\frac{1}{n}}.$$

» Ici il faut entendre par chacun des exposants fractionnaires contenus dans la parenthèse, non pas cet exposant lui-même, mais son plus petit résidu positif relativement au module n; d'ailleurs $F(\alpha)$ désigne comme $f(\alpha)$ une fonction rationnelle de α et de A, B, C, ... Cette expression de (α^m, z) étant substituée dans l'équation (5), on obtient une forme que z_x doit nécessairement avoir, et qui satisfait toujours au problème, quelles que soient les fonctions rationnelles de α et de A, B, C, ... qu'on prenne pour $f(\alpha)$ et $F(\alpha)$.

» La comparaison de ce résultat avec la forme générale donnée ci-dessus des racines d'une équation résoluble du degré μ conduit à des propositions intéressantes; mais des conséquences plus intéressantes encore se tirent de la comparaison de l'expression (8), en y supposant que A, B, C, ... soient des nombres entiers, avec l'expression correspondante que fournissent certaines équations abéliennes qui se présentent dans la théorie de la division du cercle, particulièrement avec la forme très-remarquable donnée pour (α, x) par M. Kummer (*Journal de Crelle*, t. XXXV, p. 363). Cette comparaison fournit en effet le théorème suivant, qui a lieu non-seulement pour un degré premier, mais dans tous les cas, savoir que :

» *Les racines de toute équation abélienne à coeffi-*

cients entiers peuvent être exprimées rationnellement au moyen des racines de l'unité.

» Ainsi ces équations abéliennes générales ne sont rien autre chose en réalité que les équations de la division du cercle.

» Il existe une relation pareille entre les racines des équations abéliennes dont les coefficients sont des nombres complexes de la forme $a + b\sqrt{-1}$ et les racines des équations qui se présentent dans la division de la lemniscate : on peut généraliser ce résultat et l'étendre à toutes les équations abéliennes dont les coefficients contiennent des nombres irrationnels déterminés et racines d'équations algébriques.

» J'ajoute encore une remarque : si l'on applique à la forme (3) le théorème précédent sur les racines des équations abéliennes à coefficients entiers, on trouve que la racine de toute équation résoluble du degré μ à coefficients entiers peut être regardée comme une somme de racines $\mu^{\text{ièmes}}$ de nombres complexes rationnels formés avec les racines de l'unité. Ainsi la forme nécessaire et suffisante la plus générale de toute racine d'une équation résoluble du degré μ à coefficients entiers s'exprime au moyen de ces nombres complexes : toutefois, la recherche effective de cette forme exige une suite de propositions sur les nombres qui dépasseraient les bornes de cette communication. »

FIN DU TOME SECOND.

10961 Paris. — Imprimerie de GAUTHIER-VILLARS, quai des Augustins, 55.



